論文 / 著書情報
Article / Book Information

題目(和文)	光学的暗号化手法を用いた生体認証に関する研究
Title(English)	Study on biometric authentication based on optical encoding techniques
著者(和文)	竹田賢史
Author(English)	Masafumi Takeda
出典(和文)	学位:博士（工学）, 学位授与機関:東京工業大学, 報告番号:甲第9882号, 授与年月日:2015年3月26日, 学位の種別:課程博士, 審査員:山口　雅浩,小林　隆夫,熊澤　逸夫,伊東　利哉,小尾　高史,生源寺 類
Citation(English)	Degree:, Conferring organization: Tokyo Institute of Technology, Report number:甲第9882号, Conferred date:2015/3/26, Degree Type:Course doctor, Examiner:,,,,,
学位種別(和文)	博士論文
Type(English)	Doctoral Thesis

TOKYO INSTITUTE OF TECHNOLOGY

Interdisciplinary Graduate School of Science and Engineering
4259 Nagatsuda, Midori-ku, Yokohama 226-8503, Japan

学位論文

光学的暗号化手法を用いた生体認証に関する研究

Study on biometric authentication based on optical encoding techniques

指導教員　山口 雅浩　教授

東京工業大学大学院 総合理工学研究科
物理情報システム専攻

竹田　賢史
Masafumi Takeda

第１章　序論

第１章では、本研究の背景、目的を述べる。また、本研究の流れ、論文の構成について解説する。

1.1　研究背景・目的

我々の生活の中で、サービスの不正な利用を防ぐために個人の正当性を確認する個人認証の技術を利用する機会は多い。例えば、入退室管理、銀行口座の開設、パソコンへのログインなど、さまざまな場面において個人認証が必要になる。近年では、電子商取引やネットワークでの情報管理などインターネットを利用したサービスの著しい発展により、時や場所を選ばず、誰もが簡単に情報にアクセスできるようになった。しかし、それと同時に、他人の情報に簡単にアクセスできるという危険性も増加し、悪意のある第３者による成りすまし被害も多い。今後は、ますますインターネットを利用したサービスが増加すると予想されるため、より安全で利便性の高い個人認証技術が必要となる。

現在、個人認証技術[1]に利用されている情報は、「所有物」、「記憶」、「バイオメトリクス」の３つに大別できる。特に電子的な空間で行われる個人認証技術について考えると、それぞれ次のようなものがある。所有物を利用した認証として、IC カード[2]、磁気カードなどを利用するものがあげられる。これは、個人の認証情報を記憶したカードを所有し、その中に格納されている情報を確認することで、個人を特定する認証である。携帯性や操作の容易さ等の長所がある反面、盗難、紛失、偽造の危険性がある。記憶を利用した認証は、パスワードや暗証番号を入力することで本人であることを確認するものである。これは、直接盗まれることがなく、簡単な手段で実現できるという長所がある。しかし、本人が忘れてしまいサービスを受けられなくなったり、覚えやすい情報を使うことで他人に簡単に知られてしまったりするといった問題がある。バイオメトリクス認証[3]は個人が持つ身体的特徴（バイオメトリクス）を用いた認証である。これは、生涯不変、本人唯一の情報を利用するため、情報の保管、記憶の必要がないという利点がある。認証の精度やコストに問題も多いが、記憶や所有物を利用した認証技術に替わる、あるいは補う技術として近年注目を浴びている。

それぞれの認証技術には、メリット・デメリットが存在するため、それぞれの技術を補うために、複合的な認証手法が利用されているケースも多い。例えば、IC カード認証では、正当な IC カード所持者を確認する方法として、PIN（Personal Identification Number）とよばれるパスワードに相当する情報を利用している。サービス利用時に PIN を IC カードに入力し、正しければ IC カードが利用できるようにする仕組みが施されている[2]。これは、「所持者」と「記憶」が組み合わされたケースである。また、IC カードの所持者を確認する際

にバイオメトリクスを利用する研究もおこなわれている。この場合、バイオメトリクス認証を行うための演算負荷は大きく、PIN 照合のように IC カード内で短時間に照合することは困難であるため、さまざまな工夫をする必要がある。

指紋や静脈などの生体情報を取得する際には多くの場合において、光が用いられる。指に光を当て、その反射光や透過光を撮像素子等によってセンシングすることで、生体情報を取得している。つまり、生体認証において、光の担う役割は大きいといえる。

1.1.1 生体認証技術について

生体認証には、生涯不変、本人唯一の情報を利用するため、情報の保管、記憶の必要がないという利点がある。それに対し、生体認証技術には解決しなくてはならない課題も存在している。

１つ目の課題として、生体情報の偽造があげられる。これまでに、指紋や虹彩等を偽造し、生体情報照合装置によって受け入れられることが報告されている[4], [5], [6], [7], [8]。指紋の偽造では、残留指紋や実際の指から採取したパターンを用いて、ゴムやシリコンやゼラチンなどにより作られた偽造指紋で指紋照合装置をだますことができている[6], [7], [9]。虹彩の偽造では、虹彩を撮影した上で、その画像を紙に印刷して作成した人工虹彩により、いくつかの虹彩照合装置をだますことができている。

２つ目の課題として、認証の精度が完全でないことがあげられる。生体情報は、DNA をのぞいて、取得の度に得られる情報は同一人物であっても少しずつ異なってしまう。認証精度を高くするためには、個人特有の特徴を効率的に抽出する必要がある。精度が完全でないため、他人受入を多少許容したとしても本人受入を高くすることや、逆に本人受入を多少犠牲にしても他人をほとんど受け入れないようにすることや、２つの中間をとることが考えられる。どのような設定にするかは、実際に使用したいアプリケーションに応じて調節することになる。

３つ目の課題として、生体情報漏洩の危険性があげられる。生体情報は数に限りがあるため、パスワードなどとは異なり、容易に変更することができない。指紋や顔は外に露出している生体情報であるため、残留指紋や顔写真を用いたなりすまし等による攻撃の危険性がある。生体情報が漏洩してしまった際の危険性を低減するために、生体情報を保護しながら生体認証を行う必要がある。

本研究では、３つ目の課題である生体情報漏洩に対する危険性を低減するための、生体情報の保護について扱う。

1.1.2 光学的暗号化技術について

近年、新たなセキュリティ技術として光学的な暗号化技術が注目を集めている。これは、光学的なフーリエ変換や位相変調や干渉を応用した暗号化技術で、光の波面を暗号化している。並列処理による高速演算やホログラム化した暗号化画像の複製が困難であるといっ

たメリットが存在する。光学的暗号化手法において最も代表的な手法として、Double Random Phase Encoding (DRPE)[10], [11]と呼ばれる手法が提案されている。これは、フーリエ変換と光の位相変調を応用した暗号化手法で、フレネル変換や非整数次フーリエ変換を用いた手法など様々な改良手法が提案されている。従来の暗号理論では、鍵が 1bit でも異なると正しく復号化できないため、生体情報のような本人であっても揺らぎがある場合は適用が困難である。それに対し、DRPE は鍵に冗長性を持つため、生体情報を鍵として利用することが可能になると考えられる。また、ディジタルホログラフィーなどの技術と組み合わせることで、秘匿化した状態で情報を取得することも可能となる。

これまでに、指紋から生成した鍵を用いて光学的暗号化手法で暗号化・復号化を行う手法が提案されている[12]。この手法は、本人の指紋画像でのみ復号化可能な暗号を実現するものであり、バイオメトリクスのパターンマッチングによる本人認証と暗号化による情報秘匿とが統合された技術として生体情報を利用したキャンセラブルな認証システム、IC カードの所持者認証[12]、暗号鍵の秘匿等が研究されている。本手法を既存の暗号理論に基づく認証手法などと組み合わせることで、生体情報を保護したまま認証が可能となる。しかし、本手法には、攻撃者に暗号解読の手掛かりを与えてしまっているかもしれないという課題が存在する。

また、光学的暗号化手法には、光の情報のまま直接暗号化を行うことができるという特徴がある。しかし、生体情報を鍵とする暗号化手法では、計算機上での実装が主である。生体情報を保護するという目的で、この光の特性を十分に生かした手法はまだ提案されていない。

1.1.3 研究目的

本研究では、光学的な暗号化手法を用いた生体情報の保護が可能な生体認証として、２つのアプローチの検討を行う。

１つ目は、生体情報を鍵とする暗号化手法の問題点の改善である。1.1.2 項で述べた通り、本手法は生体情報を保護したまま行う生体認証に応用可能であるが、攻撃者に暗号解読の手がかりを与えてしまっている危険性が存在している。そこで本研究では、手掛かりを与えないような平文画像・鍵画像の生成手法について検討を行い、より安全な生体情報を用いた暗号化手法の提案を行う。

２つ目は、光学的暗号化手法を別の面から応用し、光の特性を十分に生かして生体情報の保護を行う手法を提案する。本提案手法では、ディジタルホログラフィーの系を応用して光学的に Double Random Phase Encoding を構築し、生体情報のセンシングを行い、生体情報を光学的に暗号化した状態で取得することを目指す。センシングを行う段階で取得する情報が光学的に暗号化されているため、計算機には秘匿化した状態で生体情報が取り込まれる。生体情報の形状が画像として電子データ化される従来のセンシングと比較し、生体情報の漏洩に対する危険性を低減できると考えられる。

1.2　本論文の構成

図 1.1 に本論文の構成図を示す。第 2 章では、生体情報を鍵とする暗号化手法の問題点に対する検討、改善手法の提案、実験による効果の確認を行う。第 3 章では、ディジタルホログラフィーの系を用いた Double Random Phase Encoding による生体情報のセンシングについて述べる。第 4 章では、本研究で提案する手法の応用例について検討を行う。第 5 章では、本論文の結論を述べる。

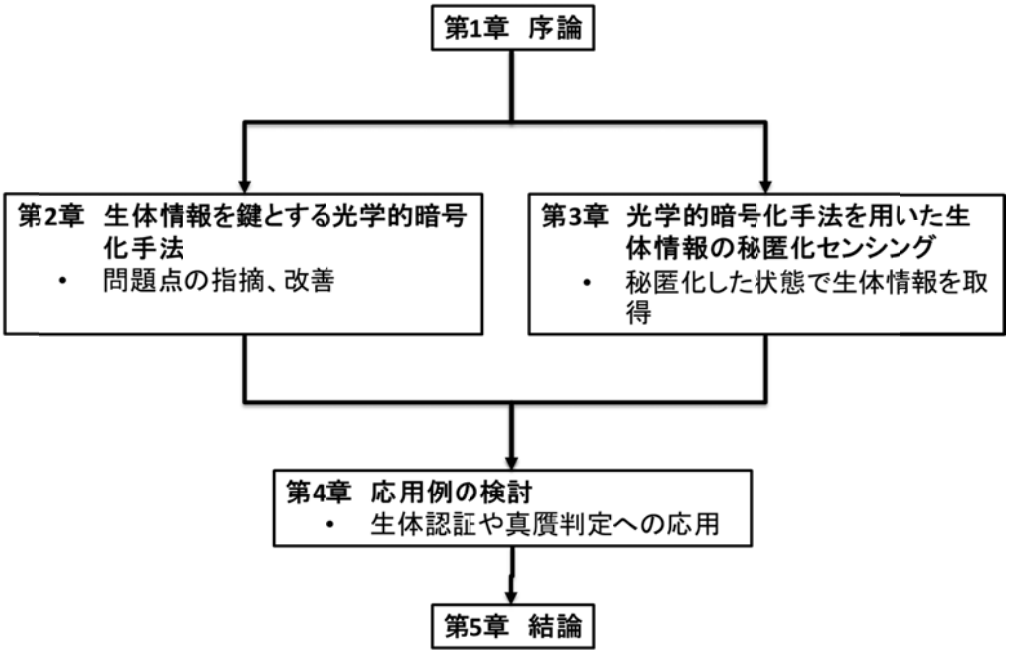


図 1.1　論文の構成

第２章　生体情報を鍵とする光学的暗号化手法

Double Random Phase Encoding (DRPE)に代表される光学的暗号化手法は、一般的なデジタルデータの暗号化技術と異なり、暗号化と復号化に用いる鍵に多少の誤差がある場合でも正しく暗号化・復号化を行うことが可能である。本章では、生体情報を鍵とする光学的暗号化手法の概要を述べ、その問題点を指摘し、解決するための手法を検討・提案、実験により、その効果を確認する。

2.1　生体情報を鍵とする光学的暗号化手法の概要

はじめに、暗号化手法の原理[5]を説明する(図 2.1)。暗号化で対象とする平文データは 2 次元空間で定義される画像である。まず、暗号化を行う元画像$f(x,y)$に対し，あるランダムパターン$R(x,y)$を変調量とする位相変調を行い、これを$f_m(x,y)$とすると以下の様に表せる。

$$f_m(x,y)=f(x,y)\exp\{jR(x,y)\} \tag{2.1}$$

そして、$f_m(x,y)$をフーリエ変換し、フーリエ変換像$F_m(u,v)$に暗号鍵画像$K_E(u,v)$を位相物体として乗算することで、暗号化画像$C(u,v)$が生成される。$C(u,v)$は以下の式で表せる。

$$C(u,v)=F_m(u,v)\exp\{jK_E(u,v)\} \tag{2.2}$$

復号化の鍵は、ホログラムから再生した暗号化画像の共役像$C^*(u,v)$に復号鍵画像$K_D(u,v)$を位相物体として乗算を行う。

$$C^*(u,v)\exp\{jK_D(u,v)\}=F_m{}^*(u,v)\exp[-j\{K_E(u,v)-K_D(u,v)\}] \tag{2.3}$$

この(2.3)式の像をフーリエ変換すると、復号化画像 $f_r(x_d,y_d)$が得られる。ここで、

$$\exp[-j\{K_E(u,v)-K_D(u,v)\}]=N(u,v) \tag{2.4}$$

とおき、

$$n(x_d,y_d)=\Im[N(u,v)] \quad (\Im[\ ]\text{はフーリエ変換演算子を示す}) \tag{2.5}$$

とすると、復号化画像$f_r(x,y)$は

$$f_r(x_d,y_d)=\Im[F_m{}^*(u,v)N(u,v)]=f_m{}^*(x_d,y_d)*n(x_d,y_d) \tag{2.6}$$

と書くことができる。ここで、*は畳み込み積分の演算子である。

この光学的暗号化手法が正しく機能するためには、正しい復号鍵で復号した場合には元

画像が正しく復元され、誤った復号鍵では、元画像が見えなくなることが要件となる。つまり、以下の式が近似的に成立することである。

$$n(x_d, y_d) = \begin{cases} \delta(x_d - \alpha, y_d - \beta) & (\text{正解の鍵を入力時}\quad) \\ random\ \ sequence & (\text{誤った鍵を入力時}\quad) \end{cases} \tag{2.7}$$

($\delta(x_d, y_d)$は Dirac のデルタ関数、αとβは復号化画像の現れる座標を表す)

この(2.7)式を満たした場合、正しい鍵を用いると、復号化画像は$f_m^*(x_d - \alpha, y_d - \beta)$となり正しい平文画像が復元され、誤った鍵を用いたときは、復号化画像はランダム画像と元画像とのたたみこみ積分となり、ホワイトノイズになる。

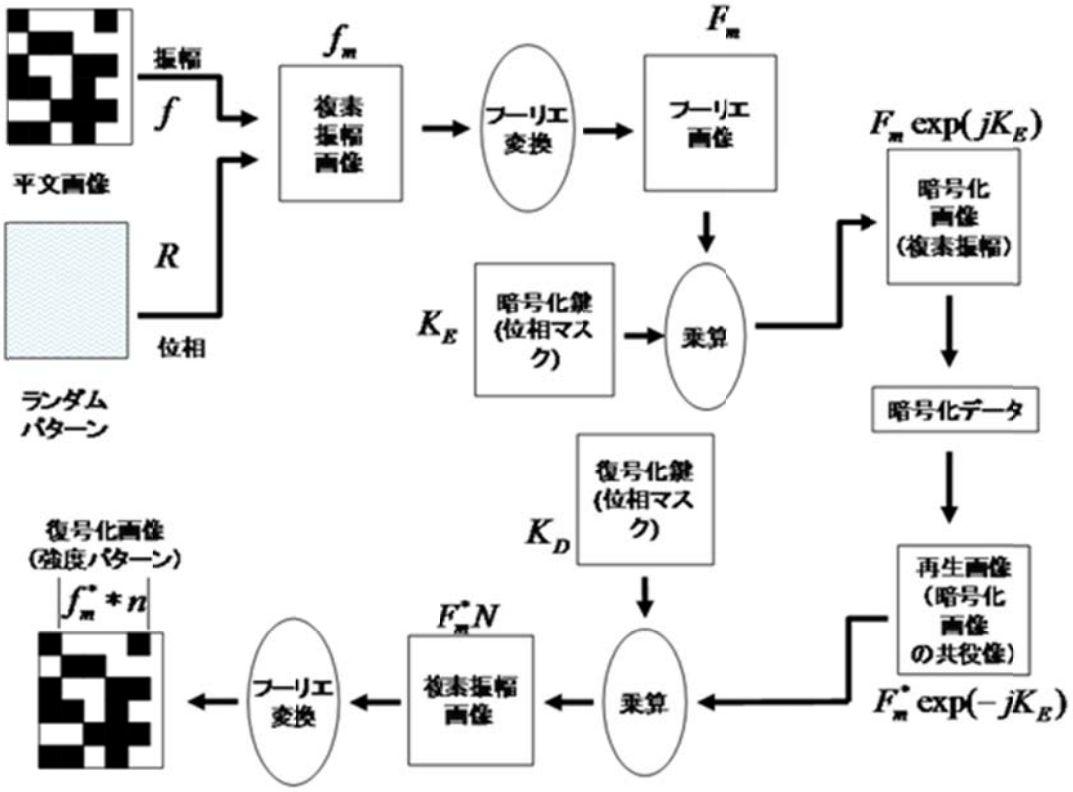


図 2.1　光学的暗号化フロー

2.1.1　鍵の要件

ここでは、本人と他人との識別性能、暗号化手法としての安全性という 2 つの面から、生体情報画像を鍵画像へ変換する際に必要な要件を述べる。まず、光学的暗号化手法を本人と他人の識別に用いるために必要な要件は、(2.7)式が近似的に成り立つことである。その

ためには、登録時と同じ生体情報を入力した場合には、$n(x_d, y_d)$に鋭いピークが現れる必要があり、登録時と異なる生体情報を入力した場合には、$n(x_d, y_d)$がランダムなパターンになる必要がある。ここで考慮すべき生体情報画像撮影時の影響としては、位置ずれ、回転、形のゆがみ、濃度のばらつき等である。

次に、暗号化画像が高い暗号強度を有するためには、光学的暗号化手法によって生成される暗号化画像が意味を持たない画像(ホワイトノイズ)になる必要がある。そのためには、暗号鍵がランダム画像(空間周波数成分の密度分布がほぼ均一)であること、画像としての空間分解能が十分に高いことが必要になる。また、鍵のビット数が多ければ多いほど、暗号解読に対する安全性は高い。また、生体情報の盗難や複製に対する安全性を考慮すると、指紋画像から暗号カギへの変換は、一方向性の不可逆変換であることが望ましい。

2.1.2 暗号鍵生成手法

現在の手法では、上述の要件を考慮した暗号鍵生成手法の 1 つとして、生体情報画像$g(x', y')$（実数）をフーリエ変換した複素振幅画像

$$\Im[g(x', y')] = A_G(u, v)\exp\{jP_G(u, v)\} \tag{2.8}$$

の位相成分$P_G(u, v)$を光学的暗号の鍵として利用することが挙げられる(図 2.2)。この手法を用いると、$n(x_d, y_d)$が暗号化の際の生体情報画像と復号化の際の生体情報画像との位相限定相関（Phase only correlation: POC）となる[13-15]ため、本人の生体情報画像同士では鋭いピークが現れ、本人と他人の場合はランダム系列に近い関数となり(図 2.3)、(2.7)式が近似的に成立する。よって、この暗号鍵を用いた暗号化手法では、位相限定相関を用いたパターンマッチングによる生体情報の照合を行うことができる。また、POC 出力と元画像との畳み込み積分が復号化画像となる。

この鍵の大きな特徴は、生体情報の平行な位置ずれに対して復号化画像が普遍性を有することである。暗号化(登録時)と復号化(出力時)で撮影される生体情報画像がシフトした場合、復号化の時の生体情報画像$g(x', y')$は、暗号化の時の生体情報画像$g(x', y')$を用いて、

$$g_S(x', y') = g(x' + \Delta x, y' + \Delta y) \tag{2.9}$$

と書くことができる。これをフーリエ変換すると、

$$\Im[g_S(x', y')] = A_G(u, v)\exp[j\{P_G(u, v) + 2\pi(u\Delta x + v\Delta y)\}] \tag{2.10}$$

となり、復号化の鍵$K_S(u, v)$は，暗号化のときの鍵$K(u, v)(= P_G(u))$を用いて、

$$K_S(u, v) = P_G(u, v) + 2\pi(u\Delta x + v\Delta y) = K(u, v) + 2\pi(u\Delta x + v\Delta y) \tag{2.11}$$

となる。よって、これらを(2.4)式の$K_E(u, v)$、$K_D(u, v)$にそれぞれ代入すると、復号化画像

は、

$$
\begin{aligned}
f_r(x_d, y_d) &= \Im\left[F_m^{*}(u,v)N(u,v)\right] \\
&= \Im\left[F_m^{*}(u,v)\exp\left[j\{K(u,v)-K_S(u,v)\}\right]\right] \\
&= \Im\left[F_m^{*}(u,v)\exp\left[-j2\pi(u\Delta x+v\Delta y)\right]\right] \\
&= f_m^{*}(x_d-\Delta x, y_d-\Delta y)
\end{aligned}
\tag{2.12}
$$

となり、生体情報がシフトした分だけ復号化画像もシフトした位置に再生像が現れる。

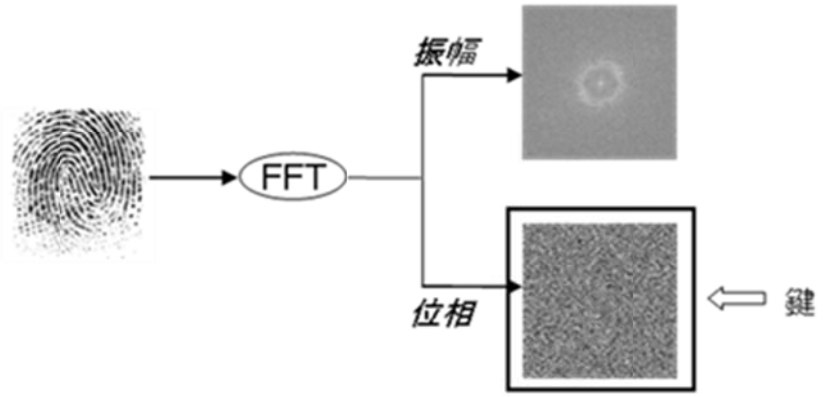


図 2.2　生体情報から鍵画像を生成する手法

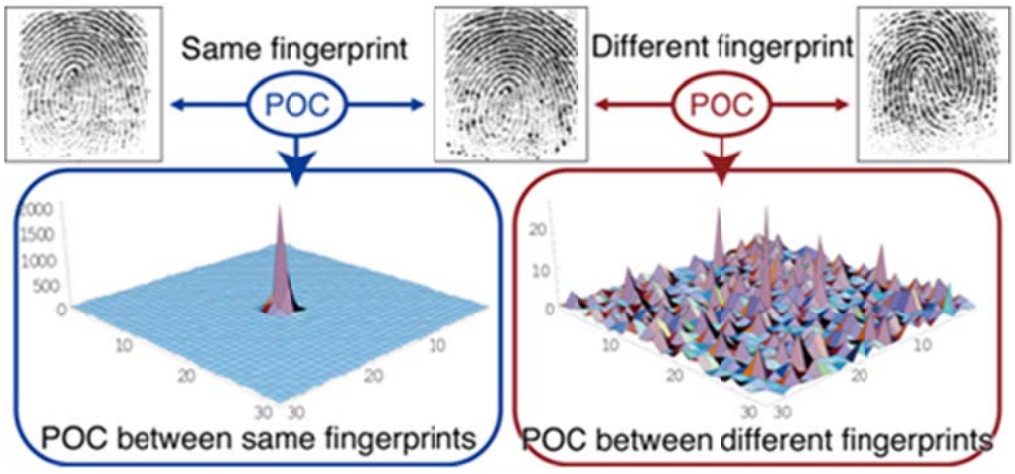


図 2.3　POC 波形の例

2.1.3　平文画像のコーディング

本手法では、任意のバイナリデータに対し暗号化・復号化を行う。光学的暗号化手法は画像を暗号化する手法であるため、認証用秘密鍵のバイナリデータを光学的暗号化に適し

た画像に変換する必要がある。その変換手法で得られた画像は、不正な照合者に解読の手掛かりを与えないために、バイナリデータの内容がどんなものであっても見た目に同様であることが望ましい。ただし、ランダムパターンのような画像に変換してしまうと、光学的暗号で暗号化→復号化された後に得られる復号化画像が元画像とほぼ完全に一致しなければならないので、本人排他率(False Rejection Rate: FRR)が著しく低下することが予想される。そこで、変換画像の画像濃度が一定であることのみを変換手法の条件とすることとし、図 2.4 に示すような方法でデータを画像化する手法を適用する。この方法では、バイナリデータのすべてのビットを 2 つのドットで表現し、右が黒ならば“1”、左が黒ならば“0”を表す。この手法は、バイナリデータの長さが一定ならば、変換された画像の濃度は一定となる。

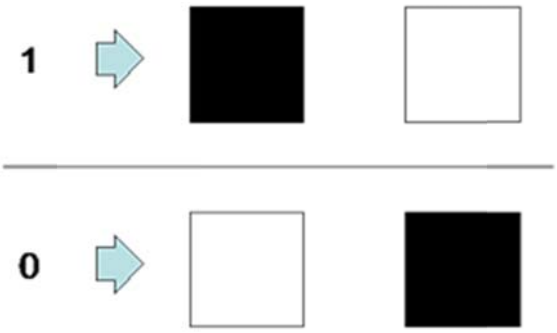


図 2.4　コーディング方法

図 2.5 に“1234ABCD”という文字列をコーディングしたビットパターン画像を示す。このビットパターン画像は、まず文字列の 1 と 0 の並びを白と黒のドットで 1 列に表現し、それを正方形になるように 2 次元に並べなおしたものである。ドットの数が正方形に合わない場合は、左上と右下に黒の正方形をパディングし、正方形にしている。

また、復号化画像から元の秘密鍵へとデコードする方法は、図 2.6 に示すように、復号化画像の中のビットパターン部分を抽出し、ビットごとに左右の画像濃度を比較し、左が大きい場合には 1、右が大きい場合には 0 としてバイナリ値を決定する。すべてのバイナリ値が決定されると照合すべき秘密鍵が復元される。このとき、復号化画像の中のビットパターンの位置は、生体情報のシフトに応じて異なる位置に出現するため、正確な出現位置を検出する必要がある。

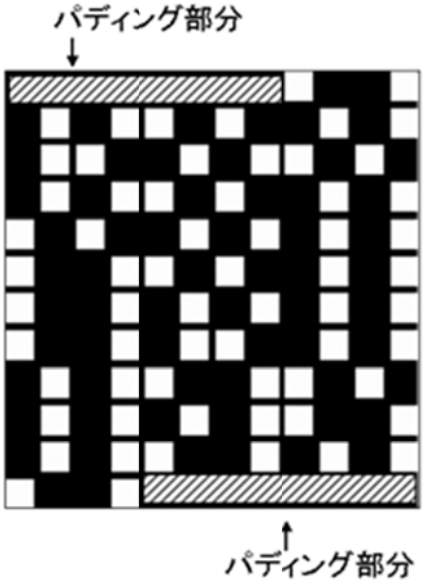


図 2.5　画像コーディング例
“1234ABCD”をビットパターン画像へコーディング

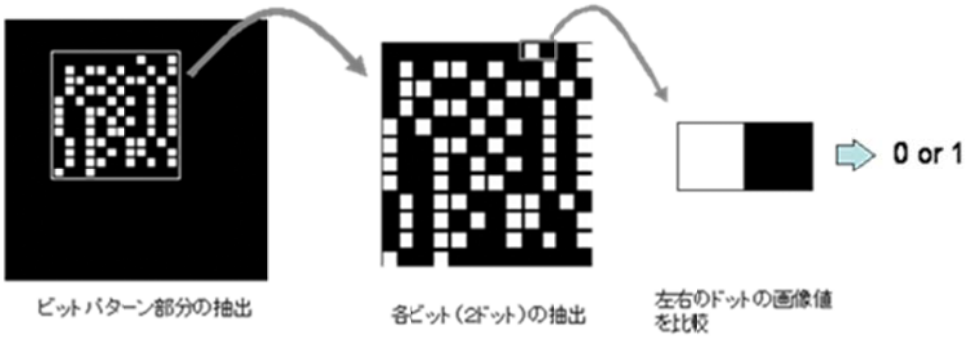


図 2.6　ビットパターン画像からバイナリデータを復元する方法

そこで、ビットパターン画像は図 2.7 に示すような位置検出用タグを設置し、このタグを利用して正確な位置を検出する。検出方法としては、復元されたタグ付きビットパターン画像とタグのみを表示した画像との相関演算を行い、相関ピークの現れる位置を求め、この位置をもとにしてビットパターン部分と推定される領域を抽出する。この流れを図 2.8 に示す。

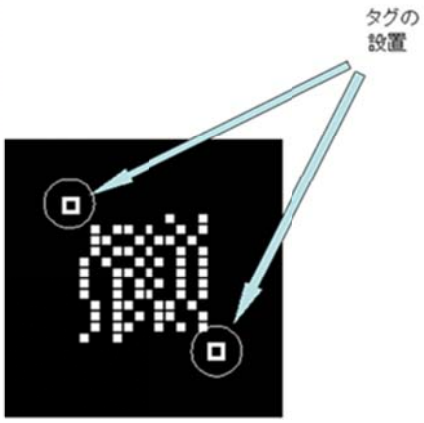


図 2.7　ビットパターンの位置を検出するためのタグの設置

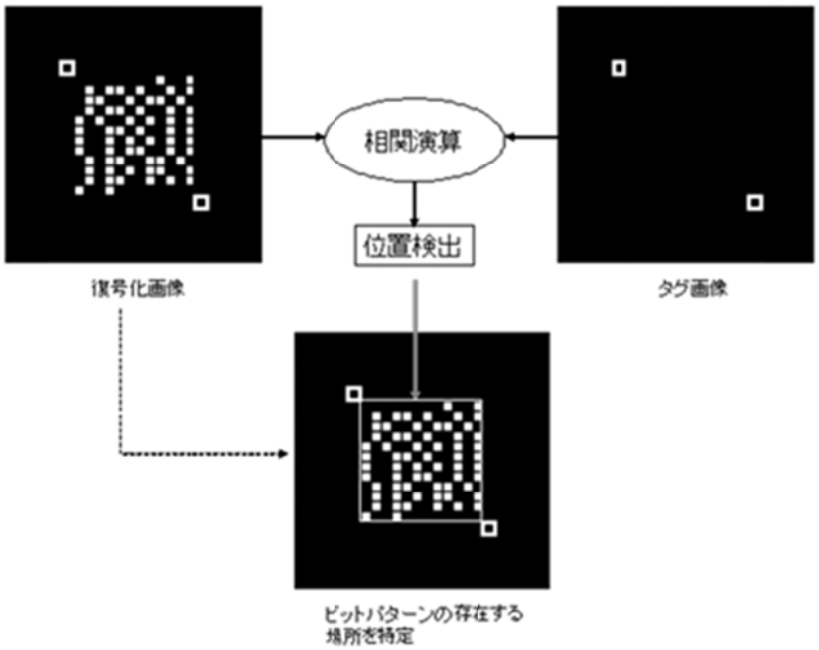


図 2.8　ビットパターンの復元位置を抽出する流れ

2.1.4　指紋の回転補正

本研究における鍵生成手法は、位相限定相関に基づいた手法であるため、回転に対して弱いという性質がある。生体情報がある程度平行移動しても正しいビットパターンが復元されるが、回転すると正しいビットパターンが得られない。

そこで本手法では、照合時に取得した生体情報画像を少しずつ回転させて複数の照合用

生体情報画像を作成し、これらをすべて入力して得られる復号化画像の中で、最もビットパターンの復号精度のよい画像を照合結果として用いている(図 2.9)。このとき、復号化画像と位置検出用のタグ画像との位相限定相関を行い、最も相関ピークの値が大きい復号化画像を、最良の照合結果として決定する。

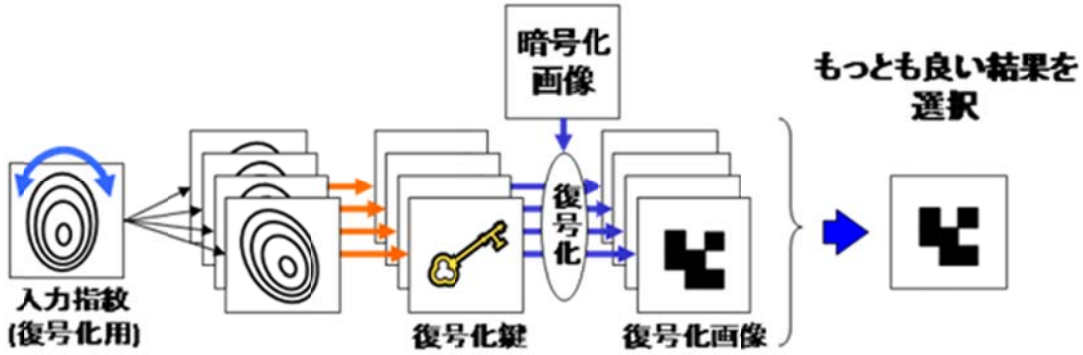


図 2.9　回転に対する対策

2.1.5　暗号化・復号化

計算機によって生体情報画像から鍵を生成し、暗号化・復号化を行った例を図 2.10 に示す。また、この時に用いた生体情報画像の POC 波形(ピーク付近のみ)が図 2.3 である。この POC 波形が$n(x_d, y_d)$ (2.7)式であり，この$n(x_d, y_d)$と元画像を畳み込み積分したものが復号化画像となる。この結果より、本人の生体情報画像同士の POC は、鋭いピークが出現してデルタ関数に近い波形となっているのに対し、本人と他人の POC 波形はほぼランダムなパターンとなっていることが確認できる。

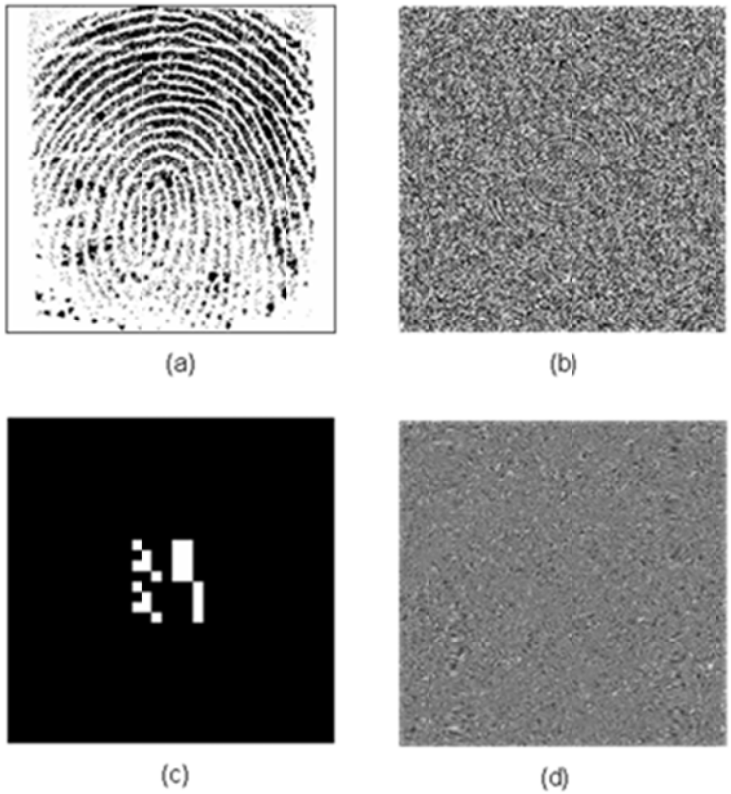


図 2.10　暗号化に用いた画像((a)暗号化に用いた指紋画像、(b)(a)から生成した鍵画像、(c)平文画像、(d)暗号化画像)

2.2　従来研究までの進捗・課題

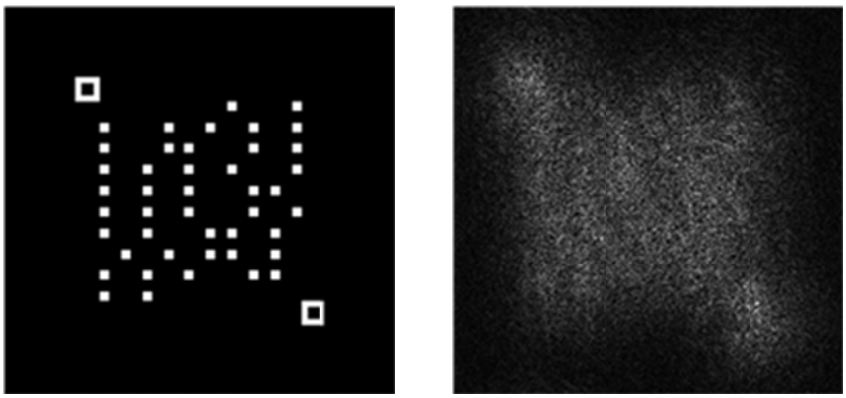
本手法の課題として、照合精度や安全性などの課題が挙げられる。照合精度に関しては、他人の生体情報を用いた際に正しく復号化できることはありえないが、本人の生体情報を用いた際に正しく復号化できない場合がしばしば存在する。そこで、鍵生成の際に生体情報の特徴領域のみを抽出したり、平文画像の生成方法を工夫したりする[]ことで、ある程度改善されることが確認されている。安全性に関しては、復号化画像や復号化過程などから攻撃者が解読の手掛かりを入手できてしまう恐れがあると考えられる。他人の生体情報を用いての復号化画像が完全なランダム画像とならずに、平文画像の影がぼんやりと見えてしまっている場合が存在する。また、復号化時の回転補正の過程において、タグとの相関ピークを手掛かりとして復号化画像を決定しているため、この情報を用いた解読を行えてしまう可能性も存在している。本研究では、これらの安全性に関する課題について検討を行い、改善するための手法の提案を行う。

2.2.1　他人の生体情報による解読の可能性について

平文画像として用いているビットパターン画像は空間分布に偏りがあるため、他人の生体情報での復号化画像であっても、ランダム画像とならず、平文画像の影がぼんやりと見えてしまう場合がある(図 2.11)。これより、他人の生体情報による復号の際において平文が解読されてしまう可能性があり、ブルートフォース攻撃に対して脆弱になっている可能性がある。

本手法は、任意のデジタルデータの暗号化・復号化に対応できるよう、デジタルデータをビットパターン画像へ変換し、この画像を平文画像として用いている。しかし、このビットパターン画像は、他人の生体情報から生成した鍵で復号化した場合でもうっすらとビットパターンが復元されており、何かしらの暗号解読のヒントを与えてしまう恐れが生じている。従来、平文画像として用いていたビットパターン画像は空間分布に偏りがあり、この影響によりうっすらと復元されてしまっていると考えられる。

そこで、空間分布に偏りのない平文画像について検討を行い、他人の生体情報での復号を行った場合でも、復号化画像から暗号解読のヒントを与えないようにすることを考える。



(a)　　(b)

図 2.11　(a)平文画像、(b)他人照合時の復号化画像

2.2.2　回転補正時の問題について

2.1.4 項にて説明したとおり、現在平文画像にタグを付加することで回転補正を行っている。この回転補正ではタグ画像と角度ごとの復号化画像の相関を計算し、その相関が最も高かった画像を復号化画像として採用している。そのため、攻撃者はタグを使用して平文画像の解読を行えてしまう可能性がある。

タグとの相関演算を行うことなく復号化を行うために、生体情報の位置・回転ずれを補

正する必要のない手法が求められる。そこで、生体情報に位置ずれや回転ずれがある場合でも、復号化画像が位置ずれすることなく、POC 波形が鋭いピークを有するように平文画像・鍵画像の改善を行う。

2.3 平文画像に関する検討

2.3.1 平文画像の要件

はじめに、平文画像の要件について整理を行う。

(1). 空間分布に偏りのない画像

(2). 振幅成分のみの画像として定義可能な画像

(3). 暗号化用生体情報と復号化用生体情報の差に対してロバストな画像

(1)について　本論文で述べる空間分布に偏りのない画像とは、平文画像中の任意の領域において、白と黒の領域が 50%ずつである画像である。

(2)について　2.1 節で述べたとおり、DRPE の平文画像は振幅成分のみの画像として定義する必要がある。もしも複素振幅画像を平文画像として用いた場合、実面で乗算したランダム位相も復号化に必要となり、利便性が下がってしまう。そこで、DRPE の平文画像は振幅成分のみで定義できる画像が望ましい。

(3)について　暗号用生体情報と復号用生体情報が完全に一致することはほとんど考えられないため、この差を吸収できるロバスト性を持つことが望ましい

2.3.2 提案手法

本研究では、提案手法として、ビットパターン画像$b(u_b, v_b)$のフーリエ変換ホログラム$B(x, y)$を新たな平文画像として採用する。本手法では振幅成分のみで定義されるビットパターン画像$b(u_b, v_b)$にランダム位相$\theta(u_b, v_b)$を乗算し、フーリエ変換を行う。フーリエ変換像の実部を取ることでフーリエ変換ホログラム$B(x, y)$を作成し、これを新しい平文画像として採用する。

$$B(x,y)=\Re\left[\Im\left[b(u_b,v_b)\exp\{j\theta(u_b,v_b)\}\right]\right] \tag{2.13}$$

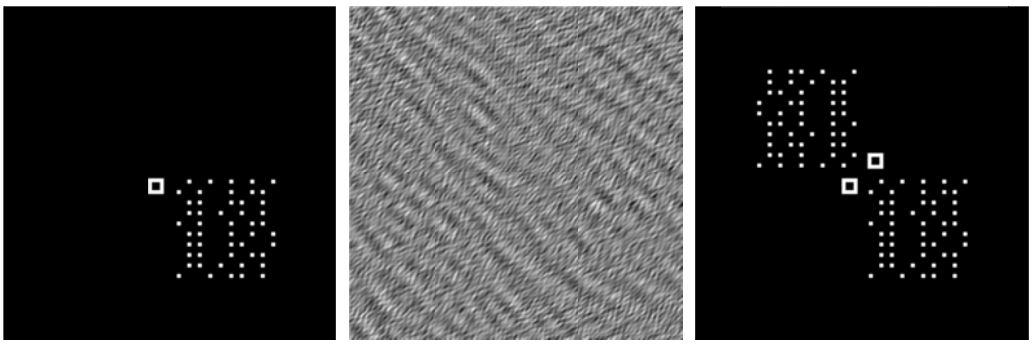
（$\Re[\ ]$は実部を取ることを示す）

生成されたフーリエ変換ホログラム$B(x, y)$は、ビットパターン画像$b(u_b, v_b)$のフーリエ変換像とランダム位相のフーリエ変換像の畳み込み積分として表わされる。ランダム位相$\theta(u_b, v_b)$のフーリエ変換像は偏りのない空間分布となるため、フーリエ変換ホログラム

$B(x,y)$も偏りのない空間分布となり、2.3.1 項で示した要件(1)を満たしている。フーリエ変換ホログラム$B(x,y)$を逆フーリエ変換することで、ビットパターン画像$b_r(u_b,v_b)$を復元することができる。しかし、フーリエ変換ホログラムはフーリエ変換後実部のみをとっているので、これを逆フーリエ変換した際の振幅画像は以下に示すような原点対称な画像となり、反転した像が足されたものになる。

$$\begin{aligned} b_r(u_b,v_b) &= \left|\Im\left[B(x,y)\right]\right| \\ &= \left|b(u_b,v_b)\exp\left\{j\theta(u_b,v_b)\right\} + b(-u_b,-v_b)\exp\left\{-j\theta(-u_b,-v_b)\right\}\right| \end{aligned} \tag{2.14}$$

そのため、この影響を考慮してビットパターン画像$b(u_b,v_b)$やランダム位相$\theta(u_b,v_b)$を生成する必要がある。ビットパターン画像$b(u_b,v_b)$が図 2.12 に示すような全体の半分の領域にのみ存在している場合、復元される画像は、図 2.12 に示すような画像になると考えられる。得られたフーリエ変換ホログラムを非負になるように調整することで、2.3.1 項で示した要件(2)を満たすことになる。



(a) (b) (c)

図 2.12 (a)ビットパターン画像 (b)フーリエ変換ホログラム (c)復元画像)

2.3.3 平文画像のロバスト性について

2.3.2 項で述べたフーリエ変換ホログラムによる平文画像は、図 2.12 に示すようにコントラストの低い画像となっている。このようなコントラストの低い画像の場合、生体情報の揺らぎによるノイズの影響を受けやすいと考えられる。そこで、フーリエ変換ホログラムを 2 値化することで、生体情報の差に対してロバストになるかどうかの検討を行う。2 値化を行った際の誤差を最小に抑えるために、フーリエ反復[]による最適化を行う。

2 値化は局所的判別分析に基づく手法を用いて行う。判別分析(discriminant analysis)は、2 つ以上のクラスを分類する基準を得るための教師あり学習手法であり、これを画像の 2 値化に適用したものが提案されている(大津の方法)[13]。画像を 2 値化した結果は、クラス間の分散が大きく、クラス内の分散が小さい程よいと言える。大津の方法ではこの基準に基

づいて、取り得るあらゆるしきい値 T で画像の二値化を行った結果を評価し、最も高い評価が得られた T を最適なしきい値として採用する。

次にしきい値の局所的な変化への対処を行う。対象となる画像を格子状に分割し、各部分画像に対してしきい値を求めた後、画像全体で滑らかに補間することでしきい値画像を生成する。しきい値画像を対象画像から減算し、差分画像を生成する。このとき、しきい値以下の画素値は 0 となるため、差分画像を閾値 0 で二値化することにより、画素ごとに異なる閾値で二値化を行うことができる。

(a) (b) (c)

図 2.13 (a)フーリエ変換ホログラム　(b)2 値化画像　(c)復元画像

つづいて、フーリエ反復法[14]について説明する。フーリエ反復法とは、実面やフーリエ面での振幅成分などの先見情報をもとに、フーリエ変換を繰り返すことで、実面やフーリエ面の位相成分の最適化を行う手法である。今回は 2 値化したホログラムから復元したビットパターンと元のビットパターンの差が小さくなるように以下のような手順で最適化を行う。

i). ビットパターンを作成し、ランダム位相を乗算してフーリエ変換し、実部をとる(フーリエ変換ホログラムの作成)

ii). 得られたフーリエ変換を 2 値化、逆フーリエ変換する

iii). 得られた逆フーリエ変換結果の振幅成分と元のビットパターンとの差分を求める。

(ア) この時の差分が十分に小さくなっていれば反復を終了し、2 値化したフーリエ変換ホログラムを平文画像とする

(イ) 差が十分に小さくなっていない場合、振幅成分を元のビットパターンに置き換え(位相成分はそのまま)、ii).に戻る

図 2.14 にフーリエ反復法で得られる画像を示す。

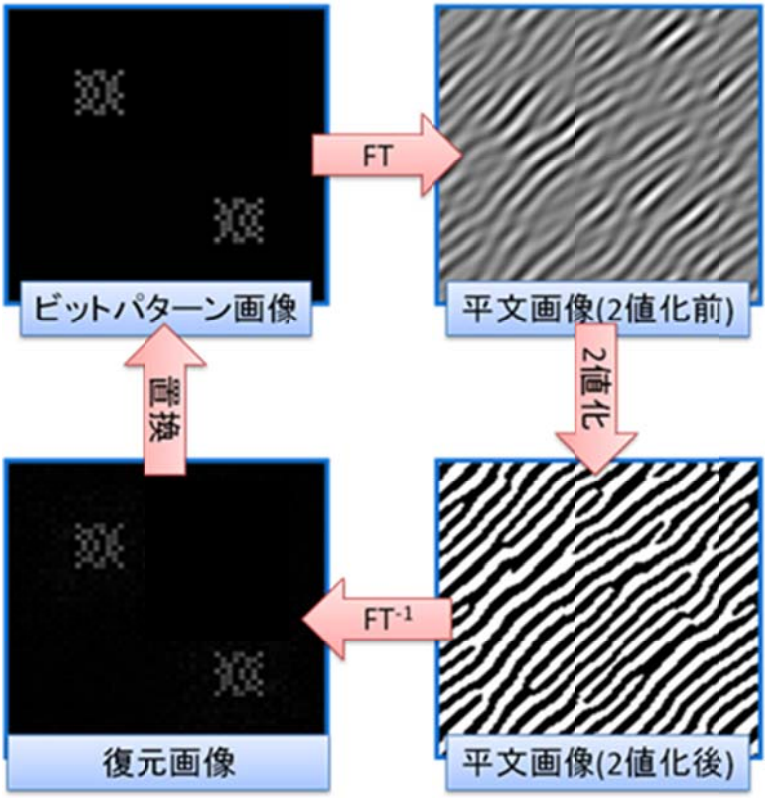


図 2.14　フーリエ反復法によるホログラムの最適化

フーリエ反復法による効果を確認するために、反復毎のビットパターン画像と復元画像の誤差を調べた。その結果を図 2.15 に示す。

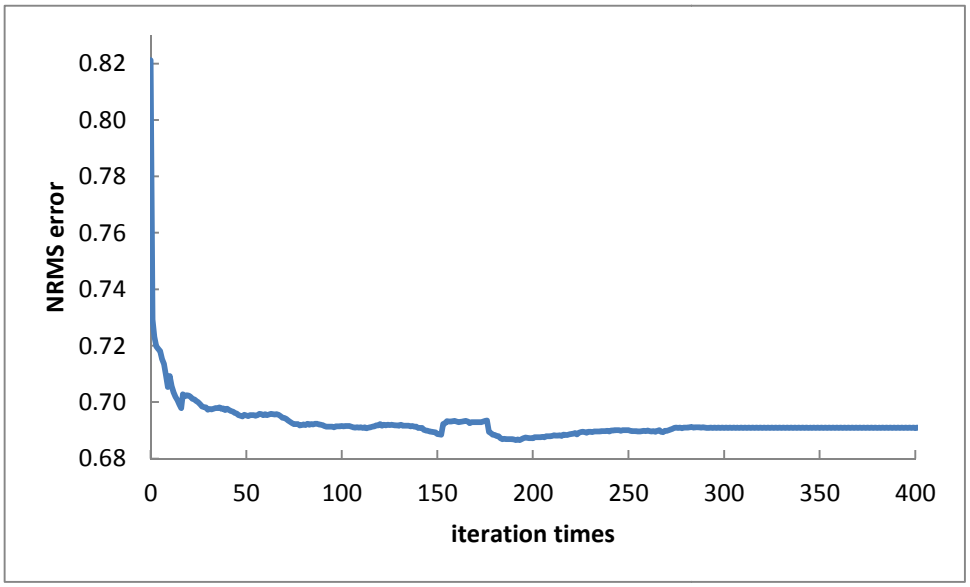


図 2.15　最適化中の NRMS

以上より、フーリエ反復を行うことで、2 値化の誤差を抑えられていることが確認できる。

2.3.4　生体情報画像のシフトについて

2.2.2 項で述べたように、暗号化用生体情報と復号化用生体情報の間に位置ずれが存在した場合、復号化画像も同様にシフトした位置に現れる。しかし、鍵の位置ずれによってフーリエ変換ホログラムがシフトした位置に現れてしまった場合でも、復元されるビットパターン画像は位置ずれのない画像として復元される(図 2.16)。これは、式(2.6) より明らかである。つまり、フーリエ変換ホログラムを平文画像として採用することによって、位置検出が不要になるというメリットも得られる。これは、次節で述べるタグを除去するために必要な条件となる。

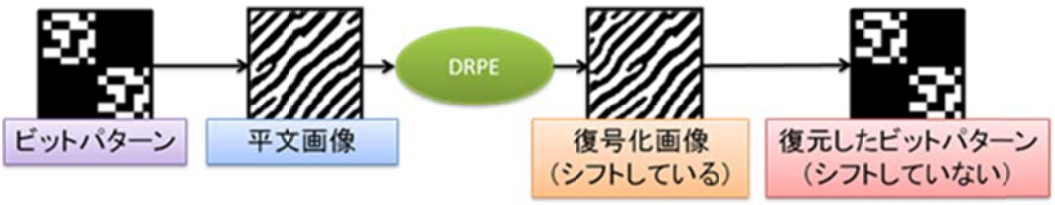


図 2.16　シフトについて

2.4　回転不変暗号鍵画像に関する検討

本手法は、2.2.4 項等で述べたように、タグを用いた回転補正を行っている。回転補正では、少しずつ回転した複数の生体情報画像を用いて復号化した画像とタグ画像と相関が最も高かった画像を復号化画像として採用することで生体情報画像の回転についての補正を行い、相関ピークの位置より、生体情報画像の位置ずれについての検出を行っている。相関ピークが高い画像が復号化画像として採用されることから、攻撃者はタグとの相関ピークを手掛かりに暗号解読を行えてしまう可能性があり、本手法の安全性を低下させている恐れがある。先ほど述べたとおり、フーリエ変換ホログラムによる平文画像は生体情報に位置ずれが生じていた場合でも復元されるビットパターン画像に位置ずれは発生しない。つまり、回転補正を行わない手法を提案することで、平文画像からタグを除去することが可能となり攻撃者に与える手掛かりを減らすことができるようになる。また、回転補正を行わないことにより、復号化の際の計算量も削減できると考えられる。

本研究では、POC の線形性に着目し、生体情報フーリエ位相成分を足し合わせの回転不変暗号鍵を生成することで、回転補正が不要な手法の提案を行う。

2.4.1　暗号鍵の要件

はじめに、暗号鍵の要件について整理を行う。

(1). 生体情報画像に回転ずれがあった場合でも正しく復号できる(鋭い POC ピークが生じる)(図 2.17)

(2). 他人を排除するために、他人の復号鍵での POC はピークが低くなる

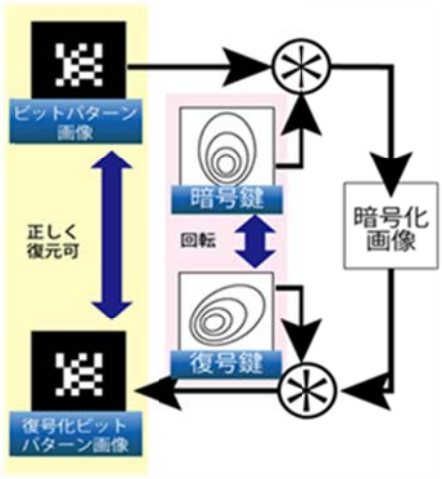


図 2.17　暗号鍵の要件

2.4.2　提案手法

2.4.1 項の要件を満たす暗号鍵として、相関フィルタの考え方を応用する。本論文では学習用データとして少しずつ回転させた生体情報画像を用意し、これらを用いてフィルタを作成する。回転した画像で学習を行うことにより、復号化用生体情報画像に回転がある場合でも鋭いピークが生じる相関フィルタとなる。代表的な相関フィルタとして、以下のものがあげられる。

(1). MACE (Minimum Average Correlation Energy)フィルタ[15]

(2). MACH (Maximum Average Correlation Height)フィルタ[16]

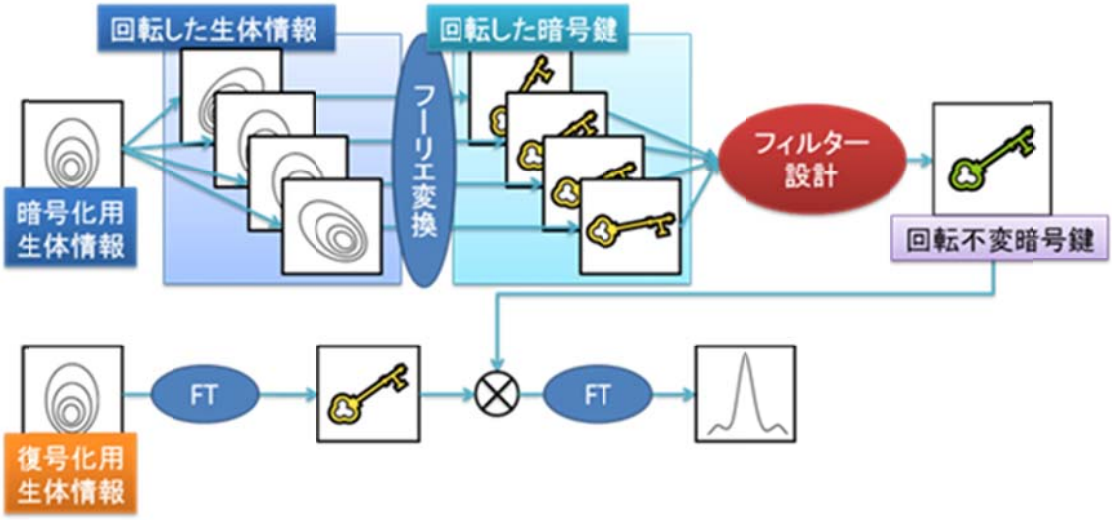


図 2.18　相関フィルタ

(1) MACE フィルタ

MACE フィルタは出力される相関ピーク値をあらかじめ定めておくという拘束条件のもと、その上で相関の平均エネルギーが最小になるように設計を行う。

$$\mathbf{X}^{*}\mathbf{h}=\mathbf{u} \tag{2.15}$$

(2.15)式は、拘束条件の式で、$\mathbf{u}$ は相関ピーク値を要素に持つ列ベクトル、$\mathbf{h}$は作成したいフィルタ、*は随伴作用素である。$\mathbf{X}$ は M 枚のフーリエ変換後の学習データ $\mathbf{x}_i$ を列ベクトルとして並べたもので、以下のように表される。

$$\mathbf{X}=\left[\mathbf{x}_1,\mathbf{x}_2,..\mathbf{x}_M\right] \tag{2.16}$$

相関の平均エネルギーは以下のような式で表される。

$$E=\mathbf{h}^{*}\mathbf{D}\mathbf{h} \tag{2.17}$$

ここで、$\mathbf{D}$ は以下のような式で表される対角行列である。

$$\mathbf{D}=\frac{1}{M}\sum_{i=1}^{M}\mathbf{D}_i,\ \mathbf{D}_i(k,k)=\left|\mathbf{x}_i(k)\right|^2 \tag{2.18}$$

ラグランジュの未定乗数法を用いて、(2.17)式 が最小になるような解 $\mathbf{h}$ を求めると

$$\mathbf{h}=\mathbf{D}^{-1}\mathbf{X}(\mathbf{X}^{*}\mathbf{D}^{-1}\mathbf{X})\mathbf{u} \tag{2.19}$$

が得られる(詳しい求め方は付録.2 を参照)。MACE フィルタは高周波領域が強調されるため、鋭いピークとなりやすいが、生体情報のゆらぎ等のノイズによる影響を受けやすい問題がある。

(2)MACH フィルタ

MACH フィルタは先ほど述べた MACE フィルタとは異なり、拘束条件を用いず、相関ピークの平均が高くなるように設計するフィルタである。

出力される相関のばらつきを定量化するために Average Similarity Measure(ASM)という以下の指標を用いる。

$$\begin{aligned}\mathrm{ASM}&=\frac{1}{Md}\sum_{i=1}^{M}\left|\mathbf{X}_i^{*}\mathbf{h}-\mathbf{M}^{*}\mathbf{h}\right|^2\\&=\frac{1}{Md}\sum_{i=1}^{M}\mathbf{h}^{*}(\mathbf{X}_i-\mathbf{M})(\mathbf{X}_i-\mathbf{M})^{*}\mathbf{h}\\&=\mathbf{h}^{*}\left[\frac{1}{Md}\sum_{i=1}^{M}(\mathbf{X}_i-\mathbf{M})(\mathbf{X}_i-\mathbf{M})^{*}\right]\mathbf{h}\\&=\mathbf{h}^{*}\mathbf{S}\mathbf{h}\end{aligned} \tag{2.20}$$

$$\mathbf{S}=\frac{1}{Md}\sum_{i=1}^{M}(\mathbf{X}_i-\mathbf{M})(\mathbf{X}_i-\mathbf{M})^{*}$$

ここで、d は画素数、$\mathbf{X}_i$ は列ベクトル $\mathbf{x}_i$ を対角行列に直したものである。また、$\mathbf{m}=\sum_{i=1}^{M}\mathbf{x}_i$ としたとき、$\mathbf{M}$ も同様に列ベクトル $\mathbf{m}$ を対角行列に直したものである。もしも、すべての相関が等しくなる場合、ASM は 0 になる。この ASM を最小にすることで、フィルタの安定性が改善される。ここで、最大化したい相関ピークの平均値(Average Correlation Height: ACH)を以下のように定義する。

$$\mathrm{ACH} = \frac{1}{M}\sum_{i=1}^{M}\mathbf{x}^{*}\mathbf{h} = \mathbf{m}^{*}\mathbf{h} \tag{2.21}$$

また、出力のノイズの分散(Output Noise Variance: ONV)も極力小さくすることを考える。ONV はノイズのパワースペクトルを要素として持つ対角行列 $\mathbf{C}$ によって、以下のように表される。

$$\mathrm{ONV} = \mathbf{h}^{*}\mathbf{C}\mathbf{h} \tag{2.22}$$

しかし、ノイズのパワースペクトルが未知の場合、$\mathbf{C} = \mathbf{I}$ (単位行列)としておく。

ASM と ONV を小さくなるようにし、ACH が大きくなるようにフィルタを設計するために、以下のような式を定義し、これが最大になるようなフィルタ $\mathbf{h}$を求める。

$$\begin{aligned} J(\mathbf{h}) &= \frac{\left|\mathrm{ACH}\right|^{2}}{\mathrm{ASM}+\mathrm{ONV}} = \frac{\left|\mathbf{m}^{*}\mathbf{h}\right|^{2}}{\mathbf{h}^{*}\mathbf{S}\mathbf{h}+\mathbf{h}^{*}\mathbf{C}\mathbf{h}} \\ &= \frac{\mathbf{h}^{*}\mathbf{m}\mathbf{m}^{*}\mathbf{h}}{\mathbf{h}^{*}(\mathbf{S}+\mathbf{C})\mathbf{h}} \end{aligned} \tag{2.23}$$

この式を最大化するは以下のように表わされる(詳しい求め方は付録.3 を参照)。

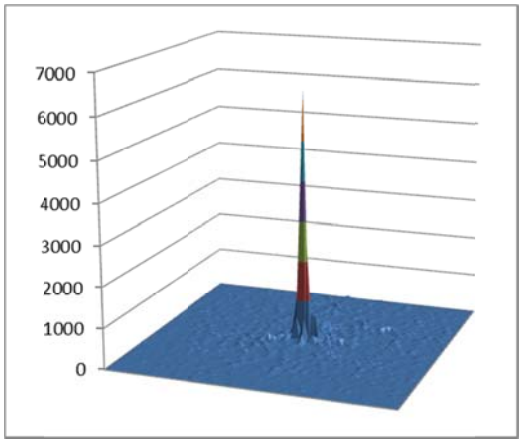
$$\mathbf{h} = \gamma(\mathbf{S}+\mathbf{C})^{-1}\mathbf{m} \tag{2.24}$$

γ は正規化スケールファクタである。

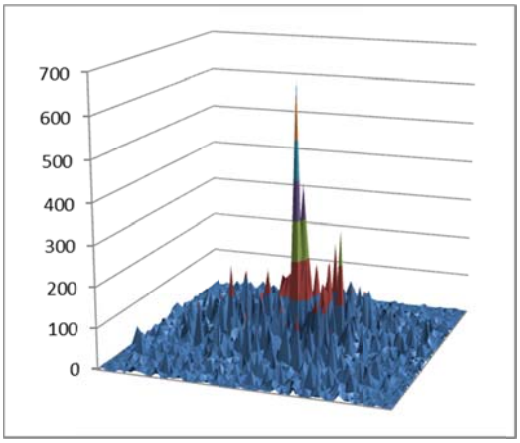
図 2.19 に、それぞれのフィルタにおいて出力される相関ピークと PSR(Peak-sidelobe ratio)[17]を示す。PSR は以下の式で表される。

$$PSR = \frac{peak - mean}{\sigma} \tag{2.25}$$

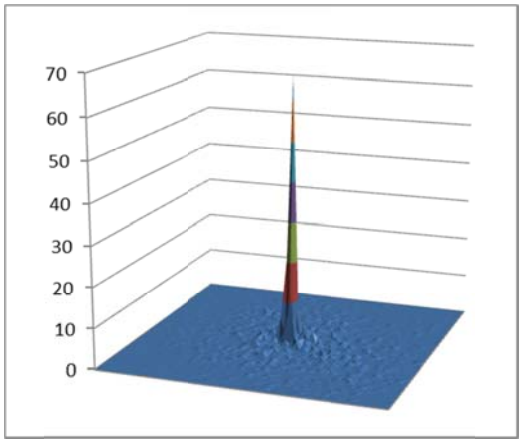
本人同士の場合、MACE でも MACH でも十分に高いピークが生じていることが確認できる。他人の場合も従来のときとほとんど遜色ない波形が得られており、PSR も従来に比べても低い値になっている(たまたま選択したものが低かっただけという可能性もあるが)。



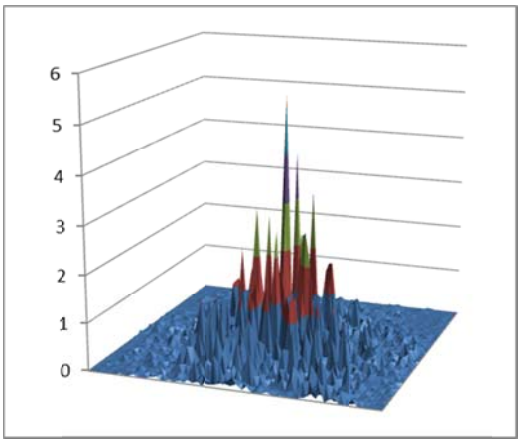
(a), PSR =0.88



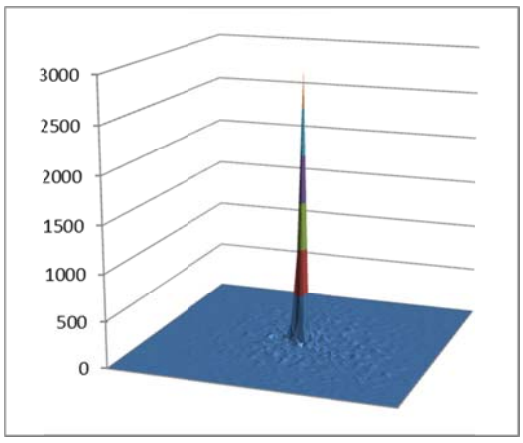
(b), PSR =0.38



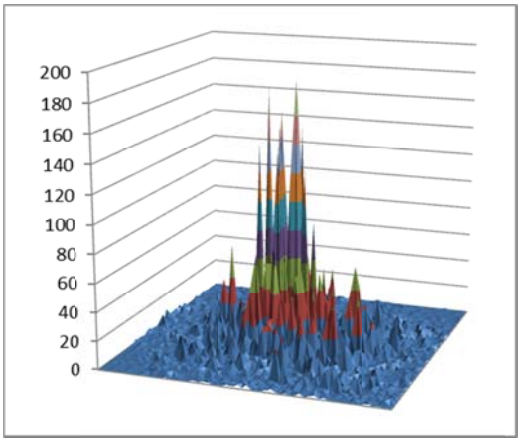
(c), PSR =0.80



(d), PSR =0.28



(e), PSR=0.77



(f), PSR=0.25

図 2.19　相関ピーク (a)本人同士、(b)他人、(c)本人同士(MACE フィルタ)、(d)他人（MACE フィルタ）、(e)本人同士(MACH フィルタ)、(f)他人(MACH フィルタ)

図 2.19 に示す POC 波形より、回転不変フィルタでも本人であれば鋭いピークが生じることが確認できる。他人の場合では完全なランダムな波形とはなっておらず、わずかながらピークが発生してしまっているのが確認できる。そのため、照合精度は若干低下するということが予想できる。

2.4.3　回転補正を行わない暗号化・復号化

フーリエ変換ホログラムによる平文画像と回転不変暗号鍵を用いて、回転補正を行わずに暗号化・復号化を行う手順を以下に示す。

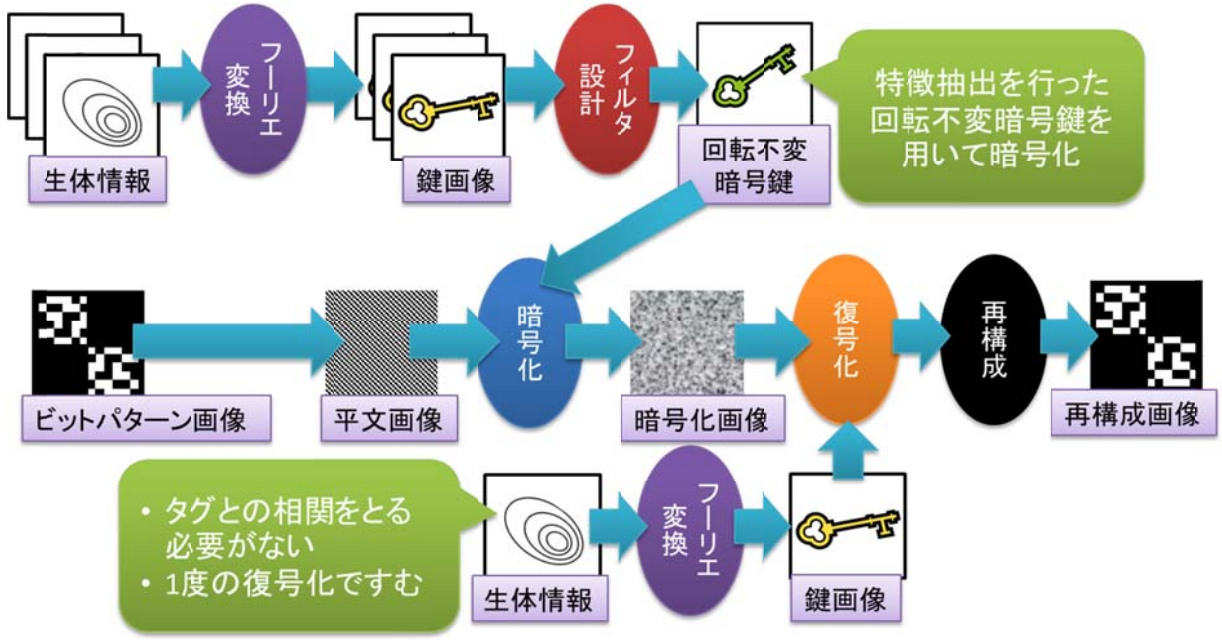


図 2.20　回転補正なし暗号化復号化

暗号化

i). ビットパターン画像からホログラム平文画像を作成

ii). 回転不変暗号鍵を生成

iii). ホログラム平文画像に対し、回転不変暗号鍵を用いて暗号化を行う

復号化

i). 暗号化画像の共役像を生成する

ii). 復号鍵を生成

iii). 復号化を行う(この際、回転補正を行わないため、タグとの相関演算を行う必要はなく、1 度の復号化ですむ)

iv). 得られた復号化画像からビットパターンを再構成する

以上のような手順により暗号化・復号化を行う。フーリエ変換ホログラムと回転不変暗号鍵を用いており位置検出や回転補正の必要がないため、タグとの相関演算は行っていない。これまでは、回転補正の際に複数回の復号化処理が必要であったが、本手法では、1 度の復号化を行えばよいことになる。その結果、計算時間を大幅に短縮できるようになる。

2.5 実験

これまで述べてきたフーリエ変換ホログラムによる平文画像や回転不変暗号鍵を用いた際の DRPE の照合精度を確認するための実験を行う。また、フーリエ変換ホログラムによる平文画像によって他人の生体情報での復号化画像のランダム性がどの程度改善したかの検証も行う。

2.5.1 生体情報画像について

本実験では、2 つのデータベースを使用して照合精度評価を行う。表 2.1 に２つのデータベースを比較したものを示す。

１つ目のデータベースは、DigitalPersona 社製の光学式指紋センサ U are U 4000 を用いて、取得したものである。指紋センサで取得される画像サイズ（解像度）は、256×256[pixel]、８ビットグレースケールの画像である。21 人から 1 人あたり２指ずつそれぞれ 10 枚の指紋画像を取得している。

図 2.21　実験に使用した指紋センサ(DigitalPersona 社製)

図 2.22　本センサで取得した指紋

2 つめのデータベースとして FVC2000 の DB2 を生体情報として用いる。FVC (Fingerprint Verification Competition)とは指紋照合の精度を競う国際的なコンペティションで、複数のセンサから採取した指紋のデータベースが参加者に配布される。このデータベースは多くの論文において手法の精度評価に用いられている。本データベースには 110 本分の指紋が各指あたり 8 枚用意されている。画像のサイズは 364×256[pixel]で、8 ビットグレースケール画像である。1 つ目のデータベースと同様に、364×364[pixel]になるように拡張し、256×256[pixel]に縮小した。各指について 4 枚の指紋画像を利用して平均画像を作成し、これより暗号化鍵を作成した。残りの 4 枚を復号化鍵とした。本人の照合を 440 パターン、他人の照合を 1100 パターン行った。

図 2.23　FVC2000DB2 の指紋

表 2.1　センサの詳細

	自前 DB(U are U)	FVC2000DB2
Subjects	42[指]	100[指]
枚数/subjects	10[枚]	8[枚]
センサ	光学式	静電容量式
画素数	256x256[pixel]	256x364[pixel]
解像度	512[dpi]	500[dpi]

2.5.2　暗号化・復号化の実験方法

暗号化・復号化の流れを図 2.24 に示す。平文は 33bit、66bit、99bit、132bit の 4 つの場合について実験を行い比較する。

暗号化の際は、各指の指紋画像のうち 4 枚の指紋画像を利用して平均画像を作成し、これより暗号化鍵を作成した。残りは復号化用の指紋とした。平均画像は **4** 枚の画像の位置と回転の向きを相関演算によるパターンマッチングで合わせ、足し合わせることで作成している。

復号化は、暗号鍵を作成した際に用いなかった指紋を用いて行った。自前の DB では本人の照合を 252 パターン、他人の照合を 1722 パターン、FVC の DB では本人の照合を 306 パターン、他人の照合を 7254 パターンの試行を行っている。

照合の評価値としては、False Rejection Ratio(FRR ; 本人だが、正しく復号化できない割合)、False Acceptance Ratio（FAR ; 他人だが、正しく復号化できる割合)とビットエラーレート(Bit Error Ratio: BER)を用いる。BER は以下の式で定義される。

$$BER=\frac{N_{Rrror}}{N_{PIN}} \tag{2.26}$$

ここで、N_{PIN}は秘密鍵のビット数、N_{Error}は復号化画像から復元した秘密鍵のエラービット数である。今回、左右の濃度値の比較で“0”か“1”かを識別するため、理論値としては、本人指紋であれば 0%、他人指紋であれば 50%となるのが望ましい。

本実験では、あるしきい値を t とした場合、BER がしきい値 t より小さければ、復号化成功とする。しきい値が t であるということは、画像化されているビットパターンのビット列の誤り訂正能力が t%であるということを仮定している。本実験では、t の値に応じて FRR と FAR を算出し、ROC カーブを描き、以下の(2.27)式によって求められる EER(Equal Error Ratio)によって、評価を行う[18]。

$$t_1=\max\{t\,|\,FRR(t)\le FAR(t)\} \tag{2.27}$$

$$t_2=\min\{t\,|\,FRR(t)\ge FAR(t)\} \tag{2.28}$$

$$[EER_{low},EER_{high}]=\begin{cases}[FRR(t_1),FAR(t_1)] & if\ FRR(t_1)+FAR(t_1)\le FRR(t_2)+FAR(t_2)\\ [FAR(t_2),FRR(t_2)] & otherwise\end{cases} \tag{2.29}$$

$$EER=\frac{EER_{low}+EER_{high}}{2} \tag{2.30}$$

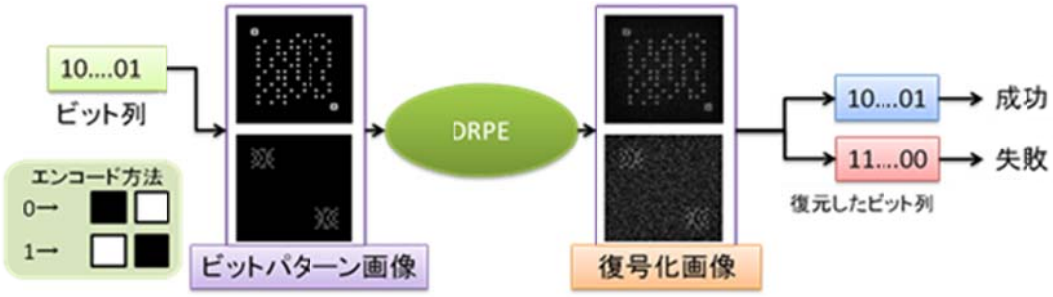


図 2.24　暗号化復号化の流れ

回転補正時の回転角とその範囲は[-10°,10°]で、1.0°間隔、合計 21 回の復号化を行う。

2.5.3　従来手法での実験結果

はじめに、従来手法での照合精度を示す。本実験では、33bit、66bit、99bit、132bit のビット列をコーディングした平文画像で実験し、比較を行う。図 2.25 に平文画像と暗号化画像を示す。

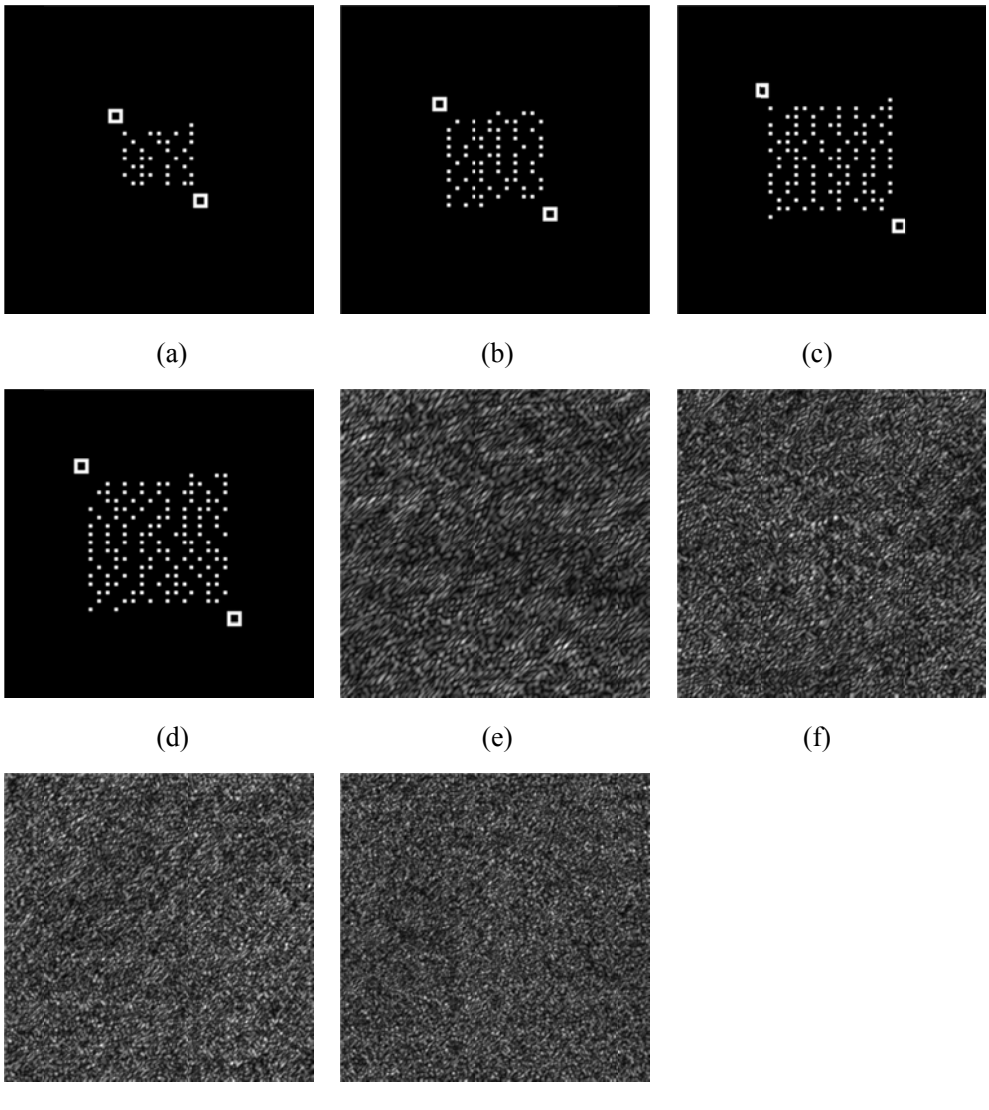
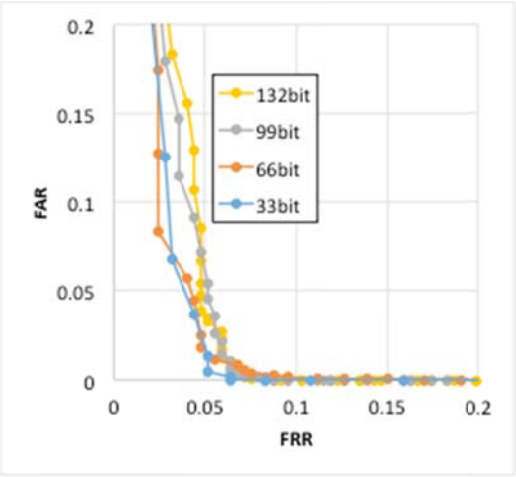


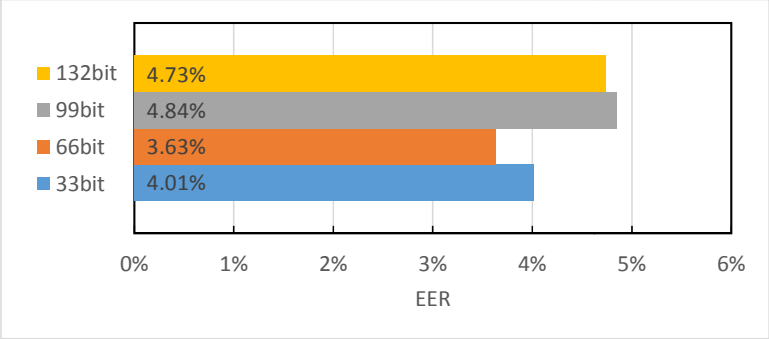
図 2.25　暗号化画像と平文画像：(a)平文画像(33bit)、(b)平文画像(66bit)、(c)平文画像(99bit)、(d)平文画像(132bit)、(e)暗号化画像(33bit)、(f)暗号化画像(66bit)、(g)暗号化画像(99bit)、(h)暗号化画像(132bit)、

図 2.26 と図 2.27 に自前 DB の場合の照合精度評価実験の結果を示す。図 2.26(a)は ROC カーブで、横軸が FRR、縦軸が FAR である。33bit や 66bit あたりの少ないビット数のほうが、99bit や 132bit あたりの多いビット数に比べ、精度がよくなっていることが確認できる。

EER で比較すると 66bit の場合が最もよい。図 2.27 のヒストグラムを見ると、ビット長が短いほど、本人 BER のヒストグラムは幅が細く、他人 BER のヒストグラムは幅が広くなり、ビット長が長くなると、逆の傾向となる。平均 BER で比較すると、おおよそヒストグラムで見られる傾向と同じである。平均他人 BER は 45%~48%の間になっており、50%からは少し離れてしまっている。図 2.28 に実験で得られた画像を示す。図 2.28 に(c)に示す他人復号化画像は BER=48.48%と 50%に近い値となっているが、これまでに述べたように、平文画像に類似したパターンがぼんやりと見えてしまっている。

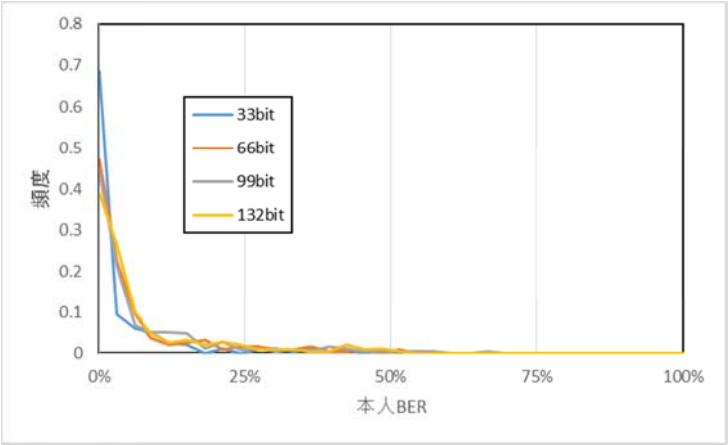


(a)

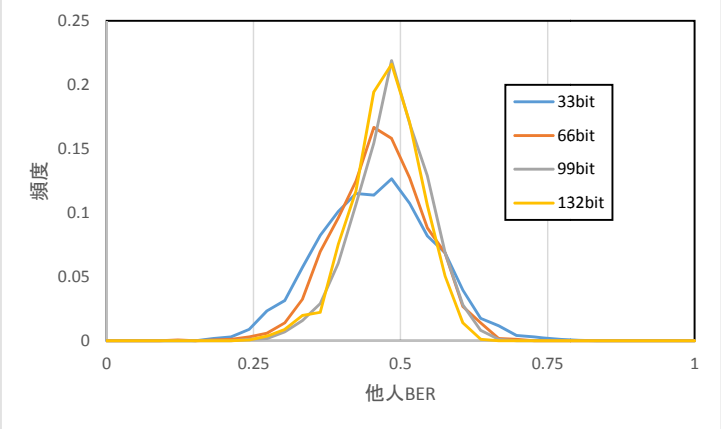


(b)

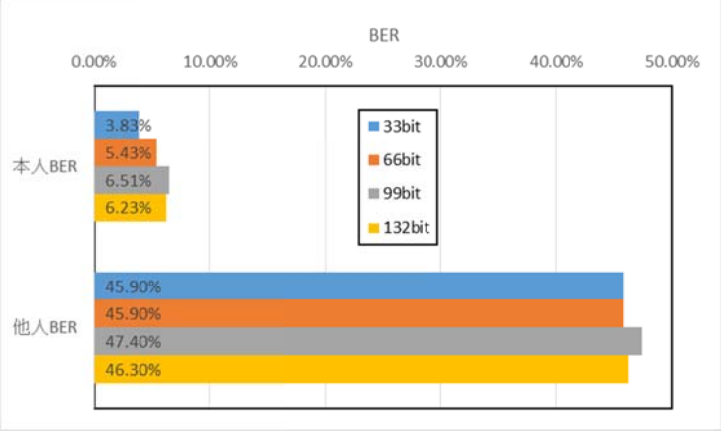
図 2.26　従来手法での照合精度評価実験結果(自前 DB)、(a)FRR—FAR の ROC カーブ、(b)EER での比較



(a)

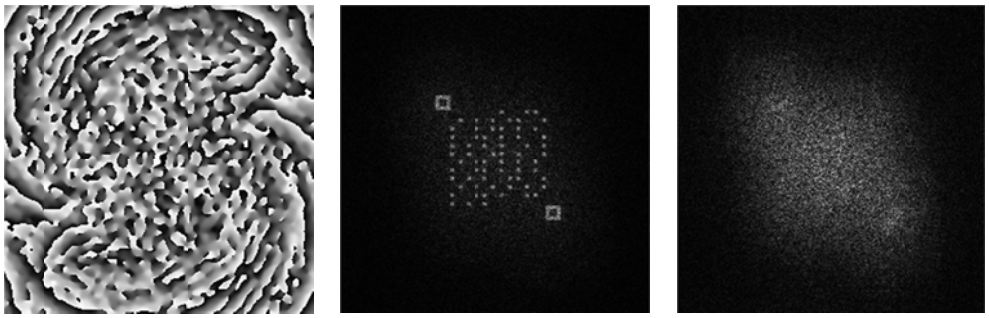


(b)



(c)

図 2.27　従来手法での照合精度評価実験結果 2(自前 DB)、(a)本人 BER のヒストグラム、(b)他人 BER のヒストグラム、(c)平均 BER

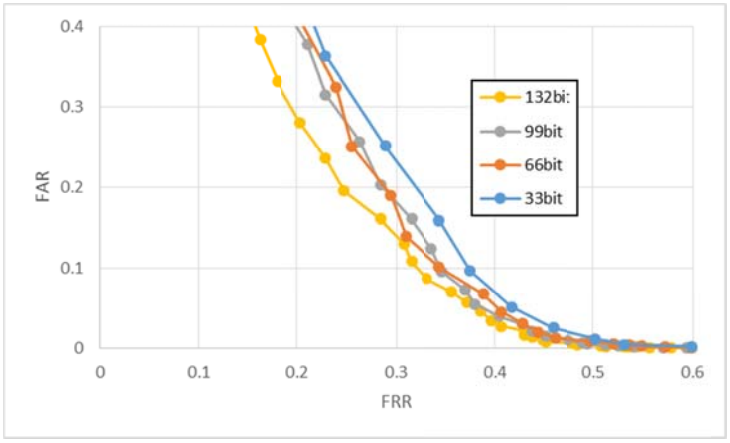


(a)　　(b)　　(c)

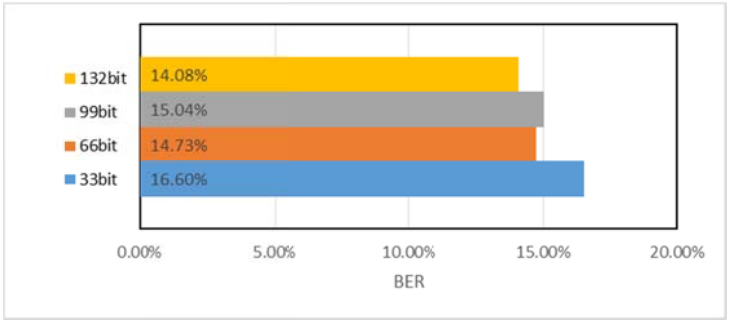
図 2.28　自前 DB での画像　(a)鍵画像、(b)本人復号化画像(66bit、BER=0.00%)、(c)他人復号化画像(66bit、BER=48.48%) 、

FVC2000 の DB2 を用いた場合の結果を図 2.29～図 2.31 に示す。でも、33bit~132bit の平文画像での自前 DB と同様の実験を行った。図 2.29(a)の ROC カーブと(b)の EER の比較より、自前の DB とは異なり、132bit のときが最も精度がよい結果となった。図 2.30 に示す BER のヒストグラムを見ると、自前 DB と同様に、ビット長が短いほどヒストグラムのピークが低いほうによる傾向が見られる。しかし、本人 BER は自前 DB のときほどビット長が短くなるとヒストグラムのピークが狭まる傾向は見られないといえる。そのため、他人 BER ヒストグラムのピークが最も狭い 132bit のときが最も精度がよくなったと考えられる。

自前 DB と FVC の EER を比較すると、それぞれ 3.63%と 14.8%であり、FVC の DB は自前 DB に比べ、大きく精度が劣っている。これは、FVC のデータベースにはあまり質の高くない指紋も多く含まれているためであると考えられる。そこで、FVC での精度を改善するために、指紋画像に処理を加えることを考える。

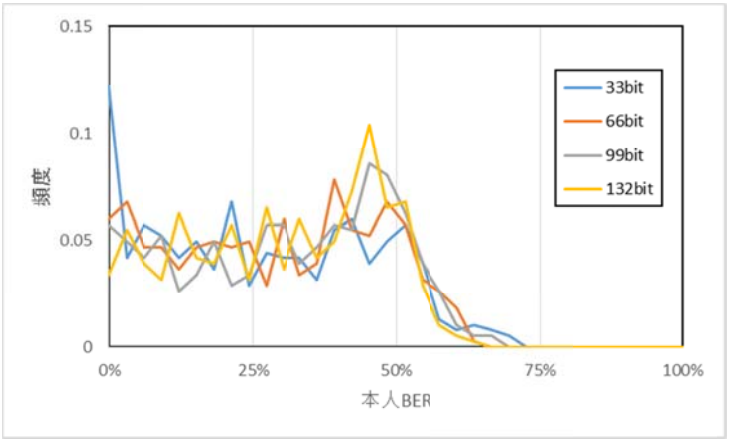


(a)

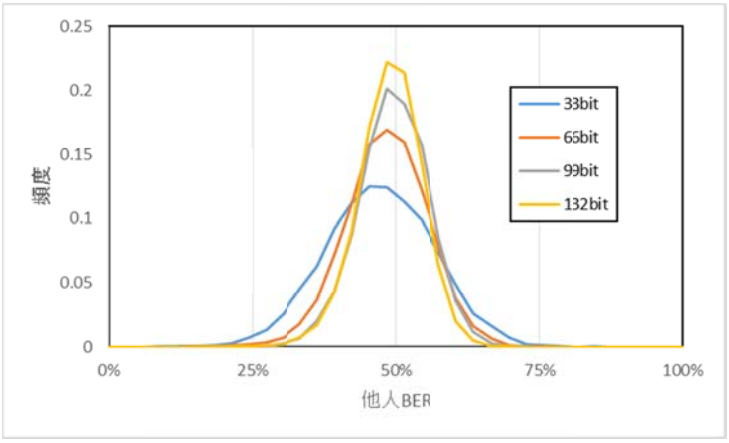


(b)

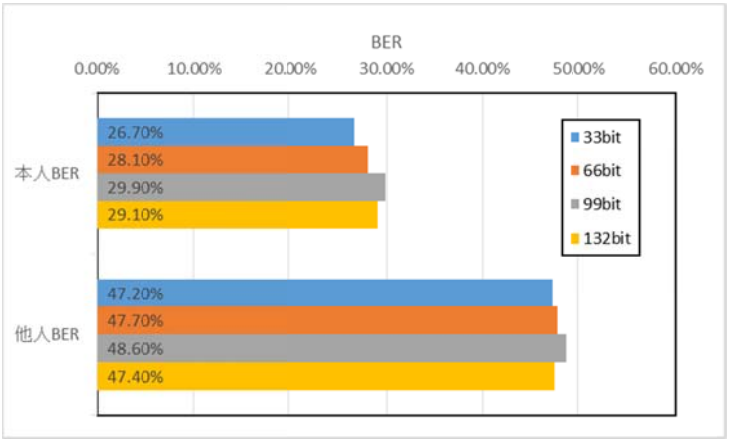
図 2.29　従来手法での照合精度評価実験結果(FVC)、(a)FRR―FAR の ROC カーブ、(b)EER での比較



(a)

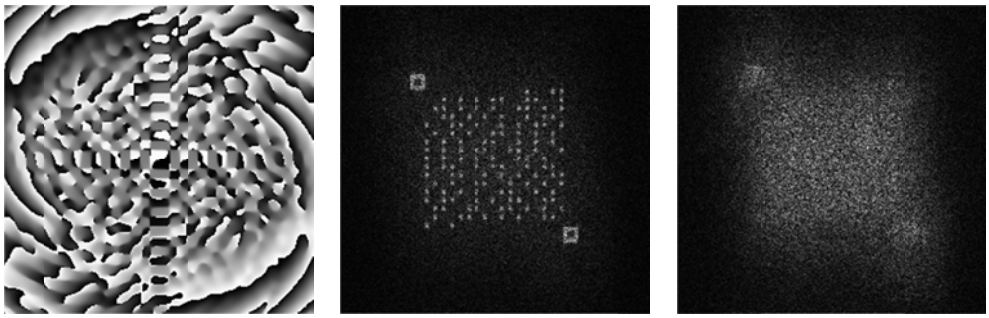


(b)



(c)

図 2.30　従来手法での照合精度評価実験結果 2(FVC)、(a)本人 BER のヒストグラム、(b)他人 BER のヒストグラム、(c)平均 BER



(a) (b) (c)

図 2.31　FVC での画像　(a)鍵画像、(b)本人復号化画像(BER=0.00%)、(c)他人復号化画像(BER=49.2%)

FVC での精度を改善するために、指紋に対して隆線強調と特異点近辺の領域を切出すという 2 つの処理を施した。

(1)隆線強調[19]

指紋の隆線を以下の流れで抽出する。

1. 指紋がある領域を抽出する。合わせて濃度の正規化を行う。
2. 隆線の局所的な向きを推定する。
3. 局所的な隆線の周波数を推定する。
4. 向きのフィルタを用いて指紋を強調する。

1. 指紋がある領域を抽出する。合わせて濃度の正規化を行う。

指紋画像の小領域ごとに分散を求め、分散の高い領域のみが通過できるようなマスクを作成する。作成したマスクと指紋画像を乗算することで、指紋がある領域を抽出する。

2.隆線の局所的な向きを推定する。(図 2.32(a))

指紋画像の x 方向の 1 階微分をf_x、y 方向の 1 階微分をf_yとし、$z = \left(f_x + jf_y\right)^2$を求める。z の位相成分が指紋画像の局所的な向きとなる。

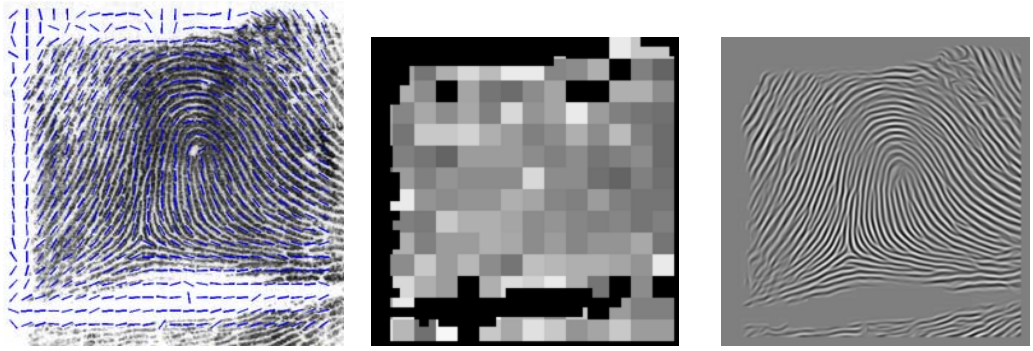
3.局所的な隆線の周波数を推定する。(図 2.32(b))

指紋の各領域に対し、向きの平均値を求める。その角度で、各領域を回転させると隆線が縦向きになる。小領域の各列を足し合わせる。グレースケールにおける膨張処理を施すことで、各列を足し合わせたものからピークになっている部分を探し出す。最初のピークの場所と最後のピークの場所の距離をピークの数で割ることで、隆線の波長を求め、その

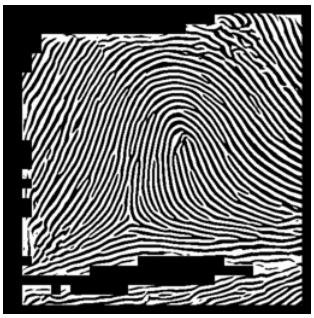
逆数が隆線の周波数となる。

4.向きのフィルタを用いて指紋を強調する。(図 2.32(c))

周波数のフィルタ内のユニークな値を取り出す。ユニークな周波数と向きに対応するフィルタを作成し、フィルタリングする。



(a)　(b)　(c)



(d)

図 2.32　隆線の強調 (a)隆線の向き、(b)隆線の局所的な周波数、(c)強調画像、(d)2 値化画像

(2)特異点周辺領域の切出し

はじめに、特異点を探し出す。指紋画像の特異点はコアやデルタと呼ばれる点で丸や三角の中心である。これを複素フィルタ[20]を用いて探し出す。向きのマップ$z=(f_x+jf_y)^2$に対し、複素フィルタを畳み込むことで、コアやデルタの位置を推定する。畳み込むフィルタは以下の式で表される。

$$h=(x\pm jy)g(x)g(y) \tag{2.31}$$

ここで、$g(x)g(y)$はガウス関数を x 方向 y 方向に分離したもので、+のときがコアの検出、-のときがデルタの検出に用いるフィルタである。

実際のフィルタリングは、向きのマップに対してガウシアンピラミッドを適用し、一番低い解像度(高レベル)の画像から始める。フィルタリング結果から最大値を探索し、次のレ

ベルでは、下のレベルで見つけた最大値の周辺を探索する。最終的にレベル 1 での最大値の場所をそれぞれコア・デルタとする。

本実験では、コアポイントを推定し、その周辺の領域を切出した。

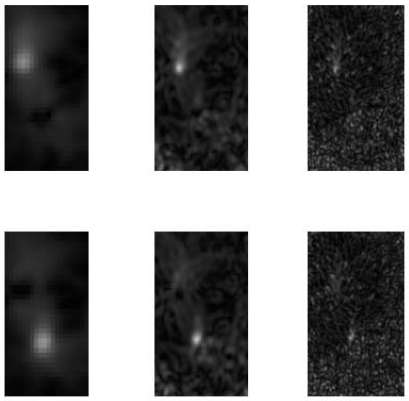
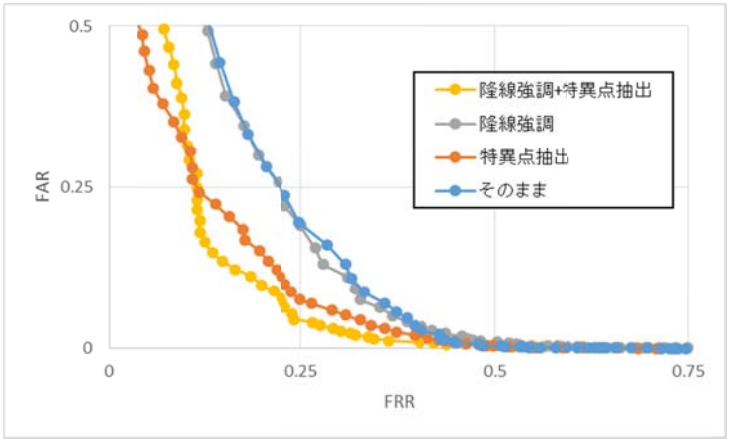


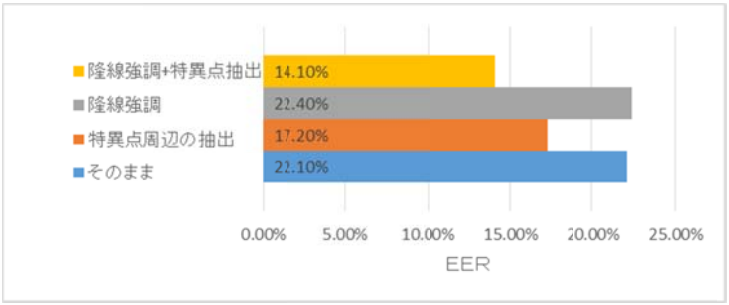
図 2.33　フィルタリング結果(左から右へだんだんレベルが下がっている、上段 : コアの検出、下段 : デルタの検出)

FVC データベースに対し、これまで述べた 2 つの処理を適用し、精度評価実験を行った。平文のビット長は 132bit に固定している。ROC カーブと EER の比較を図 2.34 に示す。隆線強調を行った場合の精度は、何もしていない状態と比較すると、ほとんど変化がないか、若干悪化している。これは、隆線強調処理により、本来隆線でないノイズ部分も強調されてしまったためと考えられる。隆線強調処理を施す際は、ノイズの影響を小さくするために、更なる前処理を加える必要がある。特異点周辺の切出しを行った場合の精度は大きく改善できている。さらに、2 つを組み合わせると更に精度が改善されている。これは、隆線強調によって謝って強調されてしまうノイズの多くは、コアポイントから離れており、切出しによって誤強調されたノイズを低減できたためであると考えられる。図 2.35 に示すヒストグラムをみると、そのままの場合と隆線強調を施した場合はほとんど変わらないが、特異点抽出を行うことで、本人・他人ともに復号化されやすくなる傾向になっていることが確認できる.

これらの処理によって、ある程度精度を改善することができたが、自前の DB と比較すると、まだまだ十分であるとはいえない。しかし、FVC のコンペ[21]では、このような質の低い指紋でも十分に高い精度で照合を行うことができる必要がある。本暗号化手法において、FVC のデータベースでも十分に良い精度を得られるようにするのは今後の課題である。

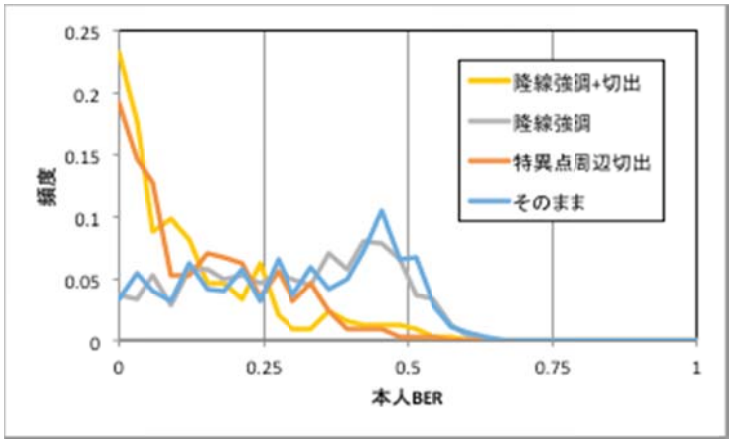


(a)

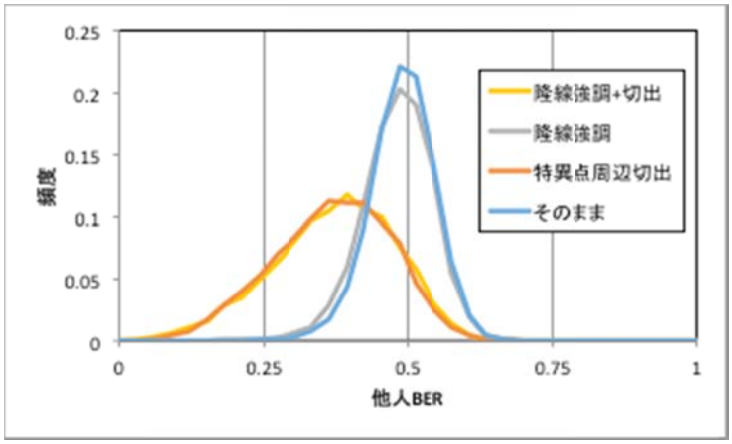


(b)

図 2.34　従来手法での照合精度評価実験結果(FVC(処理))、(a)FRR―FAR の ROC カーブ、(b)EER での比較



(a)



(b)

図 2.35　従来手法での照合精度評価実験結果 2(FVC(処理))、(a)本人 BER のヒストグラム、(b)他人 BER のヒストグラム、

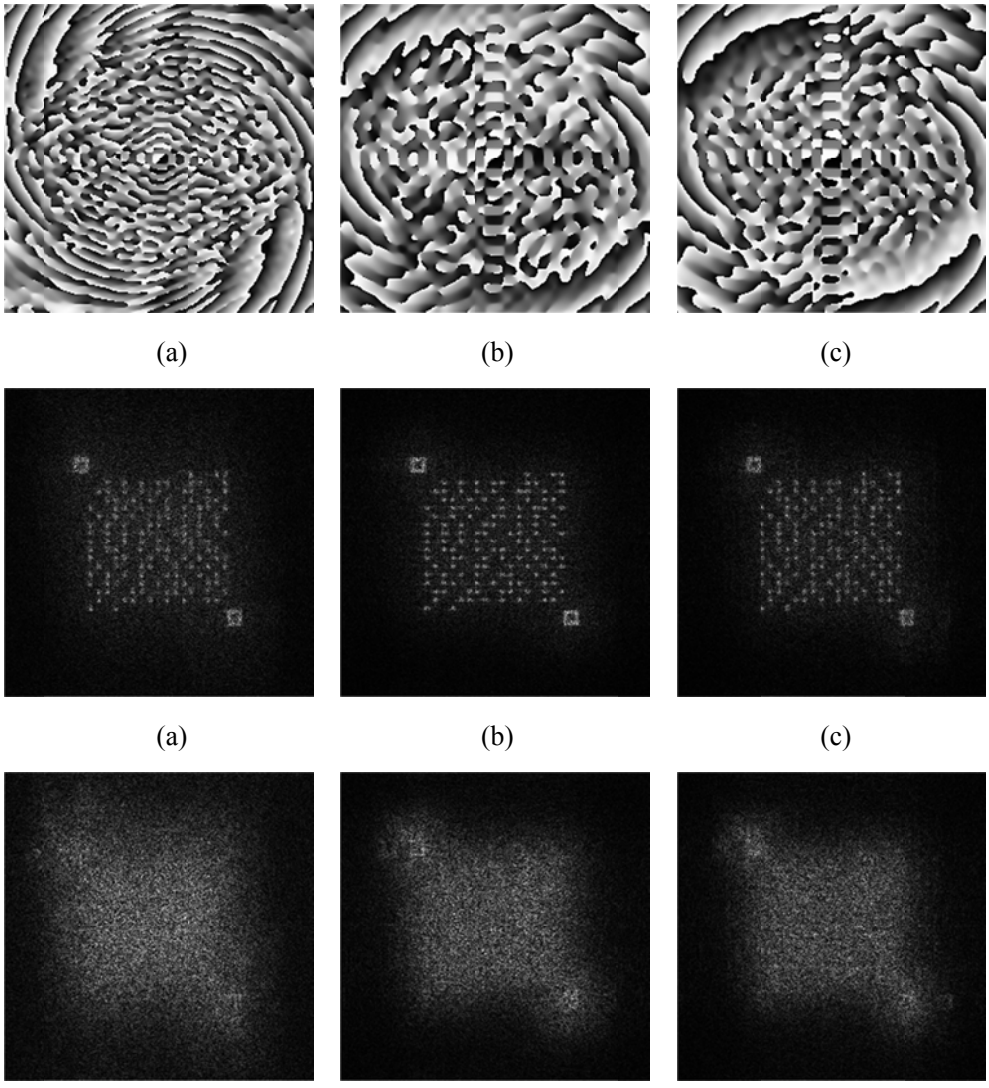


図 2.36　FVC での画像　(a)鍵画像(隆線強調)、(b)鍵画像(特異点周辺切出)、
(c)鍵画像(隆線強調+切出)、(d)本人復号化画像(隆線強調)、
(e) 本人復号化画像(特異点周辺切出)、(f) 本人復号化画像(隆線強調+切出)、
(g) 他人復号化画像(隆線強調)、(h) 他人復号化画像(特異点周辺切出)、
(i) 他人復号化画像(隆線強調+切出)、

2.5.4　ホログラムを平文画像として適用した際のロバスト性について

ホログラムを平文画像として適用した際の照合精度評価実験の前に、シフト、回転、ノイズに対するロバスト性について調査を行う。従来手法と 2 値化をしないホログラムと 2 値化を行ったホログラムでの照合精度の比較を行う。画像のサイズは 256×256[pixel]である。

図 2.29 にシフトに対するロバスト性、図 2.30 に回転に対するロバスト性、図 2.31 にシフトに対するロバスト性のグラフを示す。各グラフの縦軸は平文画像と復号化画像の相関ピークの値を示している。横軸は、シフト量、回転角度、1 画素あたりのノイズを加えた回数／100 である。加えたノイズはガウシアンノイズで、平均値 100、標準偏差 30 である。

図 2.37～39 に示す結果より、シフト、回転、ノイズどの場合においても、量が少ない場合は、従来＞2 値化前＞2 値化後の順であるが、量が多くなってくると、従来＞2 値化後＞2 値化前となっていることがわかる。これより、2 値化によりロバスト性が改善されることと従来手法の平文画像よりも劣っているということがわかる。

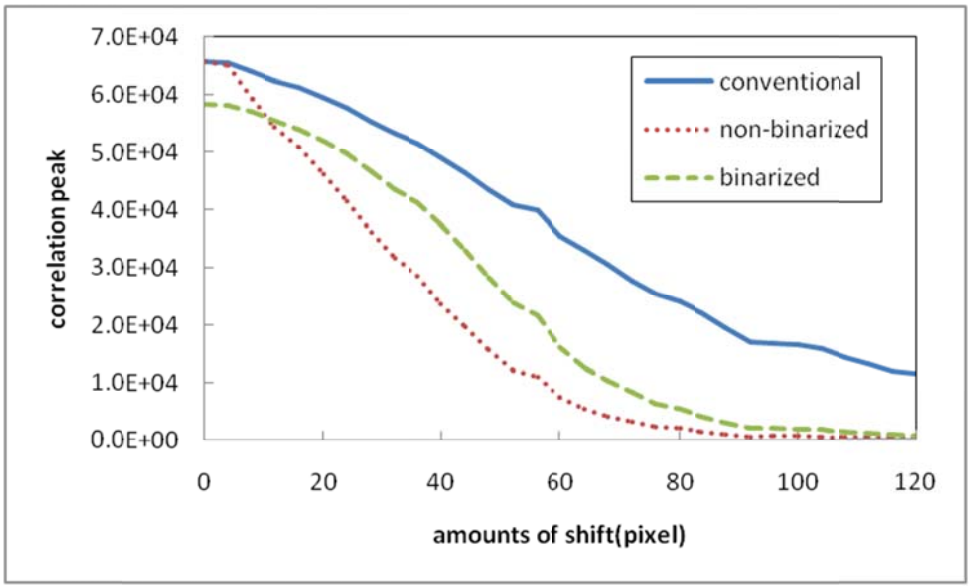


図 2.37　平文画像のシフトに対するロバスト性

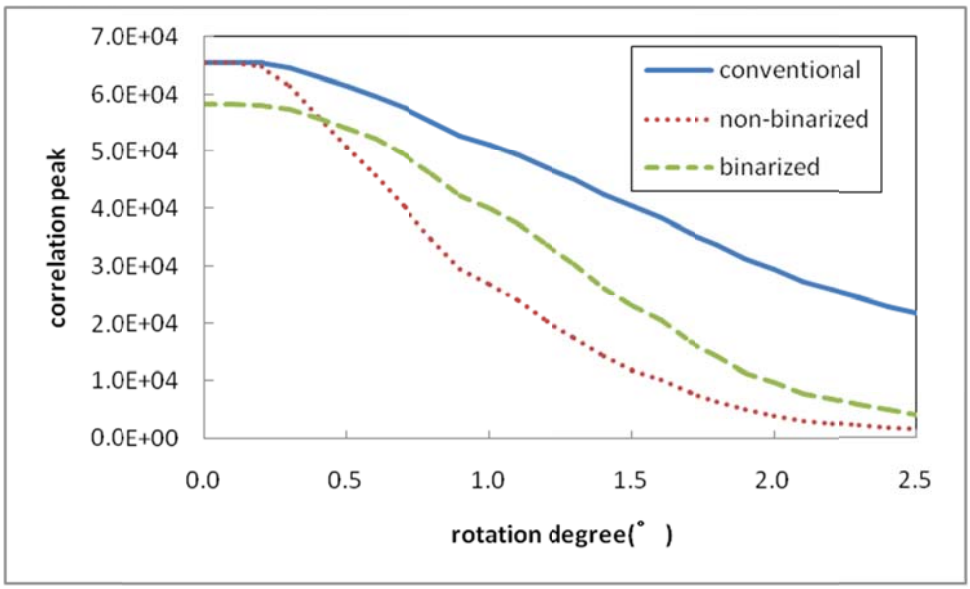


図 2.38　平文画像の回転に対するロバスト性

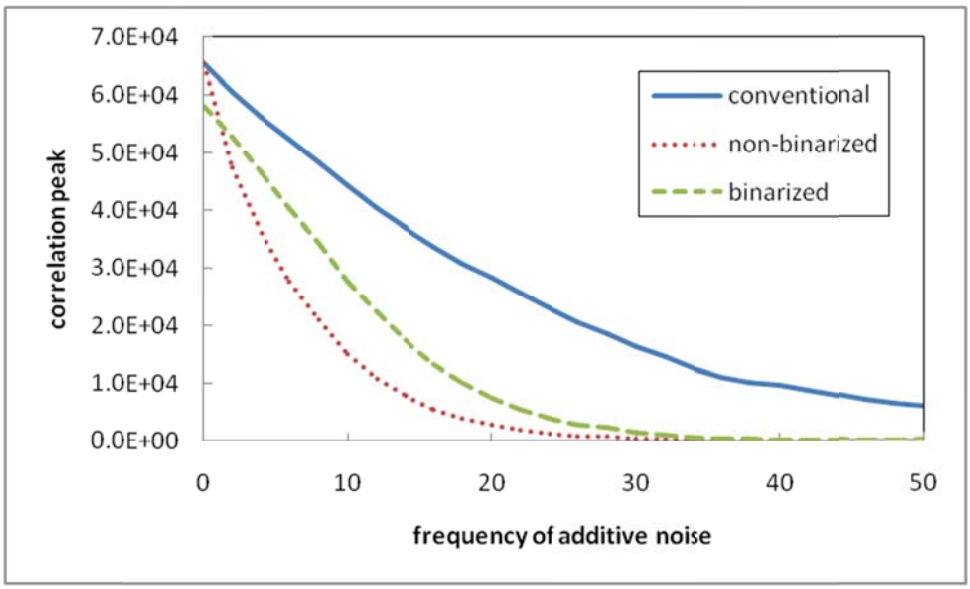


図 2.39　平文画像に対するノイズに対するロバスト性

2.5.5　ホログラム平文画像、回転不変暗号鍵を適用した際の照合精度評価実験の結果

つづいて、ホログラムを平文画像として適用した場合の照合精度評価実験を行う。ここでは、従来手法とホログラム(グレー)とホログラム(2 値化)とホログラム(2 値化)+回転不変

暗号鍵での照合精度の比較を行う。回転不変暗号鍵の生成にはMACHフィルタを採用している。また、平文のビット長は 132bit で実験を行う．実験に用いた平文画像と暗号化画像を図 2.40 に示す.

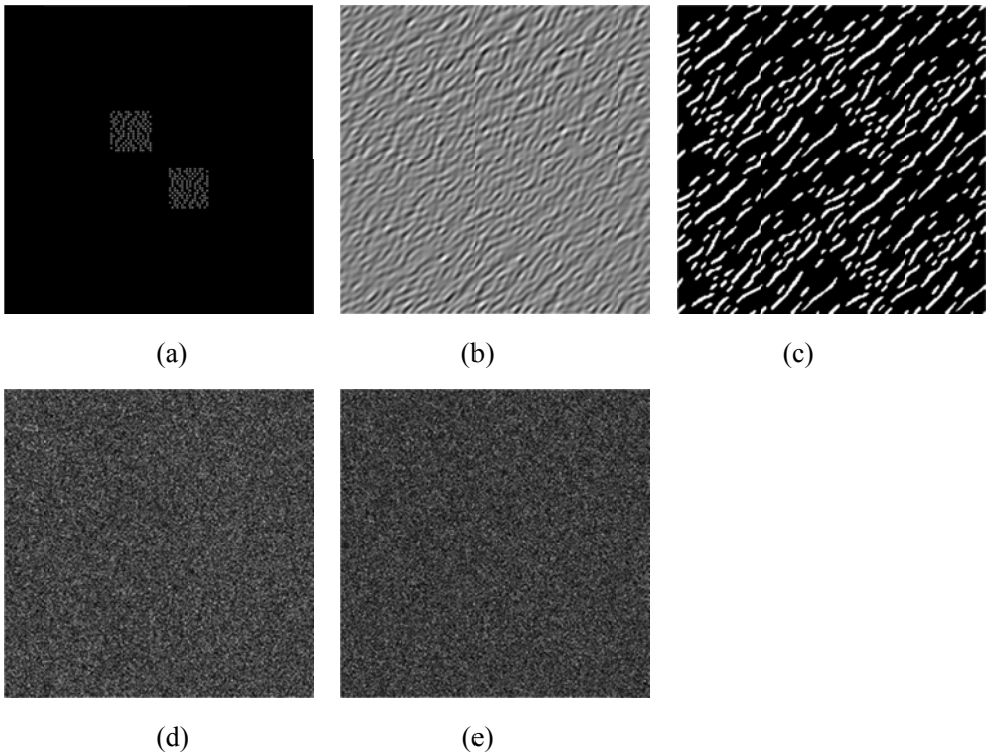
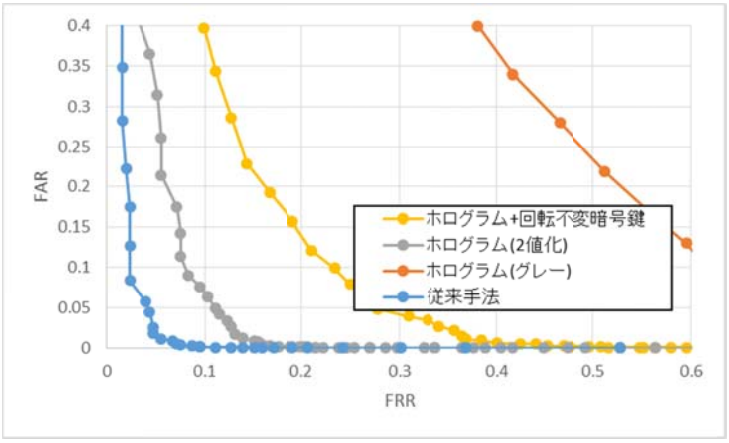


図 2.40　(a)ビットパターン画像、(b)平文画像(2 値化無)、(c)平文画像(2 値化有)、(d)暗号化画像(2 値化無)、(e)暗号化画像(2 値化有)

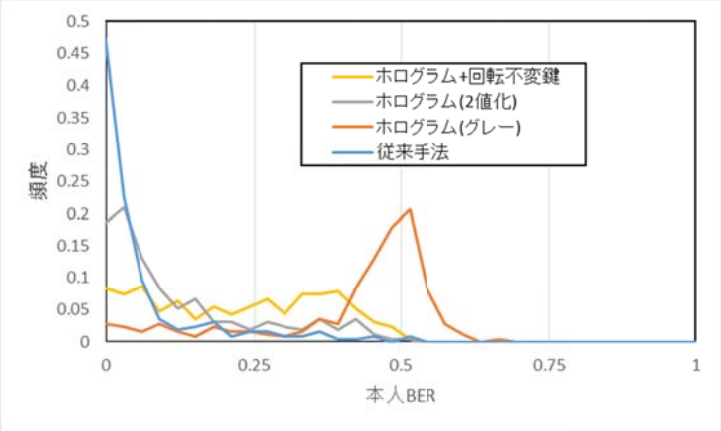
自前 DB での実験結果を図 2.41~2.44 に示す。2 値化を行っていないホログラム平文画像の場合、精度が大きく低下しているが、2 値化を行うことで、精度の低下を大きく抑えられていることが確認できる。図 2.42 に示す復号化画像を見ても、2 値化を行っている場合のほうが、再構成されるビットパターンのコントラストが高くなっている。これに更に回転不変暗号鍵を組み合わせると、ある程度は復号化できているが、従来手法等と比較すると精度は悪化してしまう。これは、2.4.2 項で示したとおり、位相限定相関のピークが少し下がってしまっていることによると考えられる。しかし、タグとの相関演算を手がかりとする解読攻撃に対する脆弱性は、解消されている。本人の BER のヒストグラムを見ると、ホログラム(グレー)の場合、ROC カーブでの結果と同様、ほとんど識別できそうにないことがわかる。他人の BER では、ホログラム平文画像を適用した場合は、2 値化濃霧にかかわらず、50%に近いところに分布している。しかし、従来手法やホログラム+回転不変鍵では、ヒストグラムは 50%から離れてしまっている。



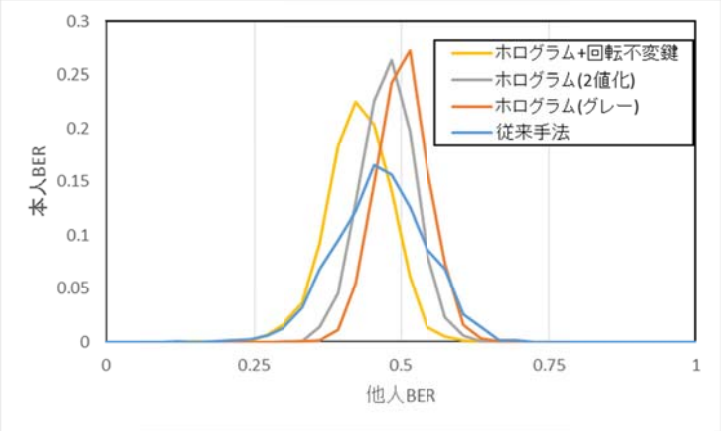
(a)ROC カーブ

(b)EER の比較

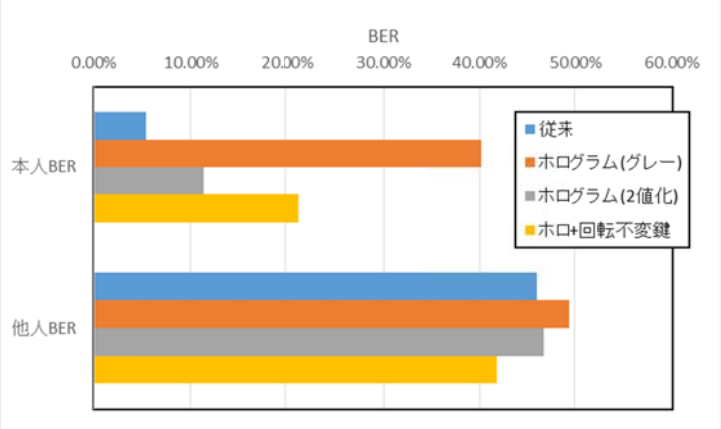
図 2.41　照合精度評価実験結果 1(自前 DB)



(a)本人 BER のヒストグラム

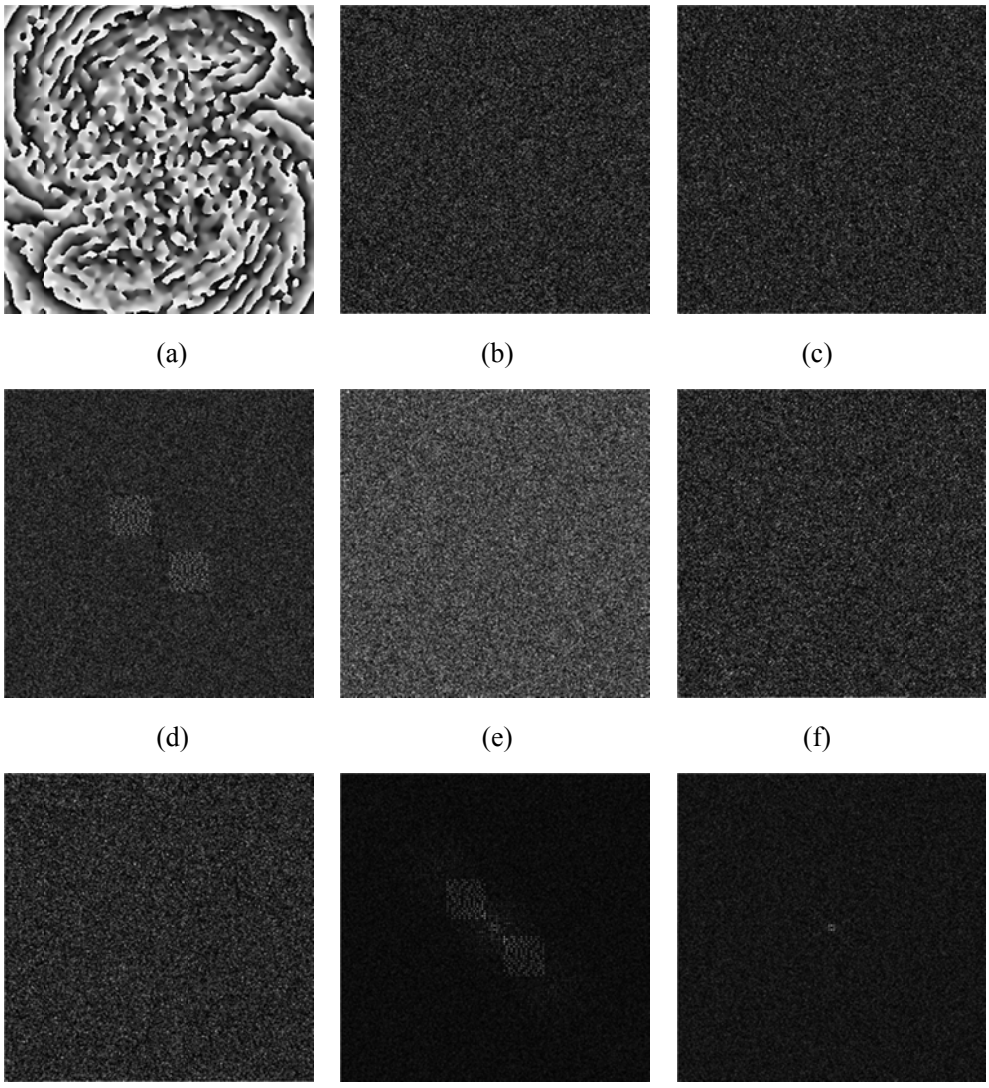


(b)他人 BER のヒストグラム



(c)BER の比較

図 2.41　照合精度評価実験結果 2(自前 DB)



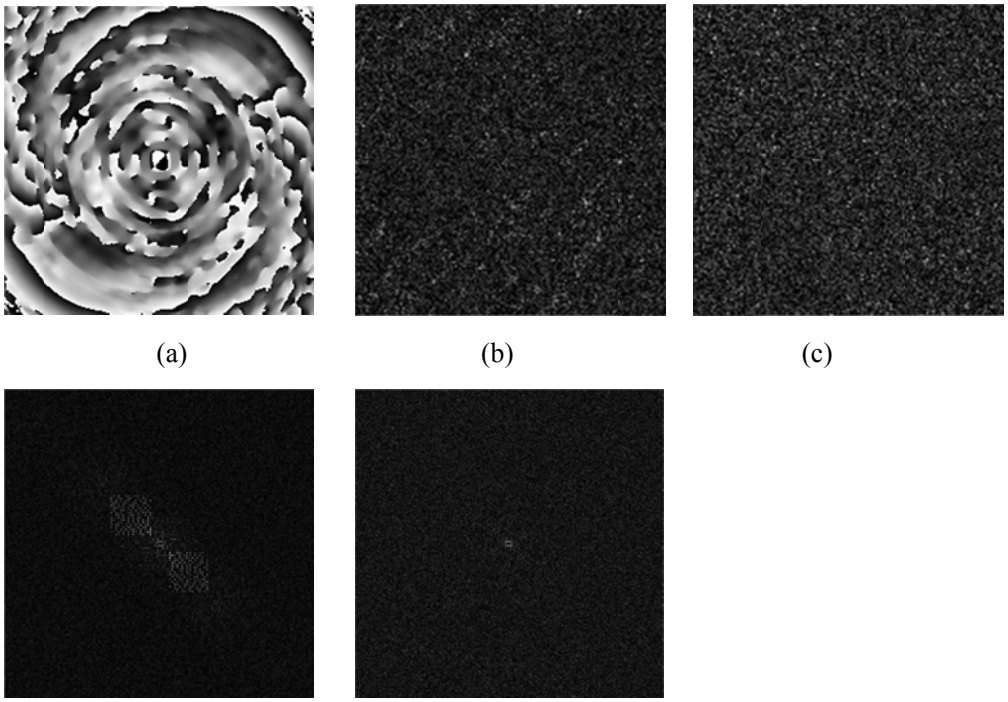
(a) (b) (c)

(d) (e) (f)

(g) (h) (i)

図 2.42　自前 DB での画像

(a)鍵画像、(b)本人復号化画像(2 値化無)、(c)他人復号化画像(2 値化無)、
(d)本人復号化ビットパターン画像(2 値化無)、(e)他人復号化ビットパターン画像(2 値化無)
(f)本人復号化画像(2 値化有)、(g)他人復号化画像(2 値化有)、
(h)本人復号化ビットパターン画像(2 値化有)、(i)他人復号化ビットパターン画像(2 値化有)



(a) (b) (c)

(d) (e)

図 2.43　画像　(a)鍵画像、(b)本人復号化画像、(c)他人復号化画像、(d)本人復号化ビットパターン画像、(e)他人復号化ビットパターン画像

2.5.6　ホログラムを平文画像として適用した際のランダム性の調査

本論文では、ホログラムを平文画像とした際に、他人の生体情報による復号化画像がどの程度ランダム画像に近づいたかを実験により調査した。実験は、図 2.44 に示すような流れで行う。ランダムパターンと他人の生体情報による復号化画像からそれぞれビット列をデコードし、BER を算出する。ランダムパターンは擬似乱数生成器を用いて作成している。これをそれぞれ複数回行い、平均 BER が等しいかどうかを検定する。平均 BER が等しい場合、他人の生体情報での復号化画像はランダムパターンになっているとみなす。

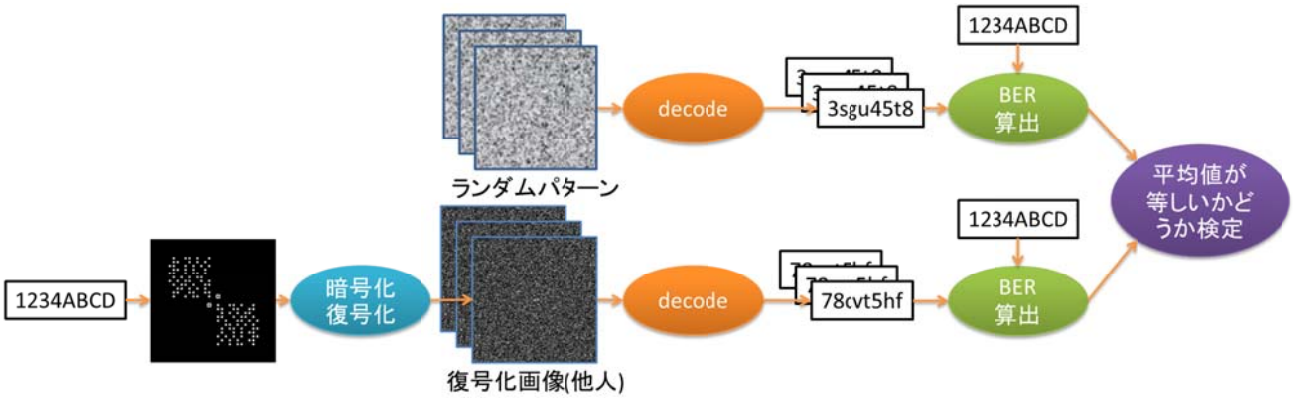


図 2.44　ランダム性の調査の流れ

つづいて、二群の平均値の差の検定を t 検定により行う。検定は以下のような前提で行う。

- 帰無仮説「ランダムパターンの BER の平均値と復号化画像(他人)の BER の平均値に差がない」、
- 対立仮説「ランダムパターンの BER の平均値と復号化画像(他人)の BER の平均値に差がある」
- 有意水準 5%で両側検定を行う。

ランダムパターンの BER の観測数をn_r、復号化画像(他人)の観測数をn_d、ランダムパターンの BER の平均値をm_r、復号化画像(他人)の平均値をm_d、ランダムパターンの BER の不変分散をu_r、復号化画像(他人)の平均値をu_d、とする。

検定統計量t_0を以下のように求める。

$$t_0 = \frac{|m_r - m_d|}{\sqrt{\frac{u_r}{n_r} + \frac{u_d}{n_d}}} \tag{2.31}$$

t_0は以下の式に示す自由度 ν の t 分布に従う

$$\nu = \frac{\left(\frac{u_r}{n_r} + \frac{u_d}{n_d}\right)^2}{\frac{{u_r}^2}{{n_r}^2(n_r - 1)} + \frac{{u_d}^2}{{n_d}^2(n_d - 1)}} \tag{2.32}$$

このとき、ν は整数にならないため、四捨五入する。有意確率 P として、自由度 ν の t 分布の$|t| > t_0$の範囲の面積を求める。有意確率 P が 0.05 以下の場合、帰無仮説は棄却され、2 つの BER 群の平均値に差があるということになり、有意確率 P が 0.05 より大きい場合、帰無仮説は採択され、2 つの BER 群の平均値に差はないということになる。表 2.4 にランダムパターンの BER 群と復号化画像 (他人) の BER 群の平均値と不偏分散、表 2.5 に各組合せでの検定統計量t_0と自由度 ν と有意確率 P を示す。観測数はすべての場合で 469 である。

表 2.4　平均値と不偏分散

	平均値 m	普遍分散 u
復号化画像(従来)	0.360	0.0132
ランダムパターン(従来)	0.496	0.00577
復号化画像(ホログラム、2 値化前)	0.500	0.00563
復号化画像(ホログラム、2 値化後)	0.492	0.00631
ランダムパターン(ホログラム)	0.499	0.00564

表 2.5　検定等軽量と自由度と有意確率

	検定統計量t_0	自由度 ν	有意確率 P	結果
従来	21.4	811	3.51×10^{-81}	差がある
ホログラム、2 値化前	0.208	936	0.836	差がない
ホログラム、2 値化後	1.49	933	0.137	差がない

以上の結果より、従来の復号化画像(他人)の BER 群の平均値はランダムパターンの BER 群の平均値と差があるとみなされる。提案手法であるホログラム平文画像の場合は、復号化画像(他人)の BER 群の平均値はランダムパターンの BER 群の平均値は差がないとみなされる。よって、平文画像としてホログラムを採用することで、他人の生体情報を用いた場合の復号化画像がランダムパターンにより近づいているということがいえる。また、2 値化を行ったホログラムでも同様にランダムパターンに近づいていることが確認できる。

2.6　第２章のまとめ

本章では、本論文で扱う生体情報を鍵とする暗号化手法について述べた。Double Random Phase Encoding と呼ばれる光学的暗号化手法の原理について述べ、暗号鍵の要件や平文画像のコーディング方法，生体情報の回転に対する補正手法等の生体情報を鍵とした場合の応用について説明した。

本手法の課題として他人生体情報での解読可能性、回転補正手法の問題があげられ、これを解決するための平文画像・鍵画像の生成手法を検討した。2.3 節では、他人の生体情報での復号化画像に平文画像のシルエットがぼんやりと見えてしまっている問題があり、平文画像の空間分布の偏りをなくすことを目的として、ビットパターン画像のフーリエ変換ホログラムを生成して、これを平文画像として用いることを検討した。生成されたフーリエ変換ホログラムはコントラストが低く、生体情報の揺らぎに対してロバストでないと考

えられるため、フーリエ変換ホログラムの 2 値化を行う。2 値化の際に生じる誤差を抑えるために、フーリエ反復による最適化を行った。2.4 節では、回転補正の問題点の検討を行い、平文画像からタグを除去するための要件の検討を行った。回転補正では、復号化用の生体情報を少しずつ回転させたものを複数用意し、それらを用いて復号した画像郡とタグの相関演算を行う。このときの相関ピークがもっとも高かった画像を復号化画像として採用している。また、相関ピークの座標によって、位置ずれ量を検出している。平文画像にフーリエ変換ホログラムを用いることで、生体情報の位置ずれ量にかかわらず、ビットパターンの出現する位置は一定となるという特徴がある。そこで、回転ずれがあった場合でも正しく復号化できる手法の検討を行った。回転ずれがあっても復号化を行うために、回転不変暗号鍵を提案し、この鍵を用いた時の位相限定相関が本人同士であれば鋭いピークが生じることを確認した。2.5 節では提案手法について照合実験を行い、精度を確認した。
また、ホログラムを平文画像とした場合の他人の生体情報による復号化画像のランダム性も調査した。 t 検定による平均値の差の検定を行った結果、ホログラム平文画像を用いた場合の復号化画像(他人)は、ランダムパターンとしてみなせることを確認した。

第３章　光学的暗号化手法を用いた生体情報の秘匿化センシング

第 2 章では、生体情報を鍵とする光学的暗号化手法の問題点を指摘し、これを改善するための手法を提案した。本章では視点を変え、生体情報を秘匿化した状態で取得することを目指す。

生体情報は重大な個人情報であり、生体情報がそのままの形で漏えいすることは決してあってはならない。従来の生体情報を取得するためのセンサは指に光をあて、その反射光や透過光を CCD などの撮像素子で画像に変換する。取得した生体情報は電子データとして存在し、登録や認証などに用いられる。電子データとして存在する以上、漏えいしてしまう危険性はあるといえる。本提案では、生体情報を取得する際の光を直接暗号化し、スクランブルされた光をディジタルホログラフィー(DH)として取得し、DH から復元した情報を用いて照合を行うことができる可能性を示す。

3.1　秘匿化センシングの概要

図 3.1 に秘匿化センシングの概要を示す。生体情報はセンサ内の光学システムにより、暗号化される。その後、暗号化された情報は認証システムに転送される。本システムの主な利点は生体情報を取得する際に生の指紋をセンシングするのではなく光学的に暗号化した DH を取得できることである(図 3.2)。ここでは、認証システムは耐タンパ性をもつなどセキュリティが保障されているものを仮定している。従来のセンシングでは、生体情報の形状を電子データとして計算機等に保存しているため、少なからず漏洩の危険性をはらんでいる。それに対し本システムでは、ディジタル化された生の生体情報は保護された認証システム内にのみ存在するため、生体情報の盗難や漏えいなどの危険性を大幅に減らすことが可能である。

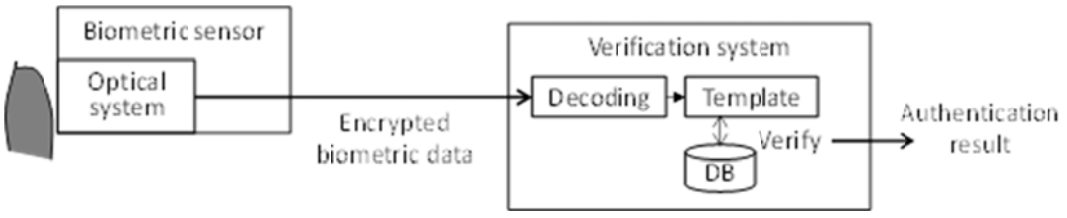
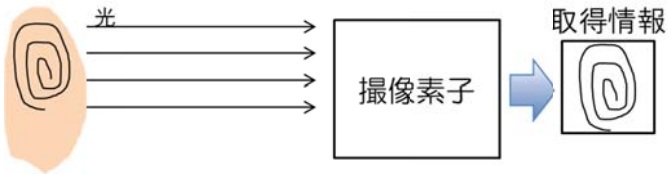
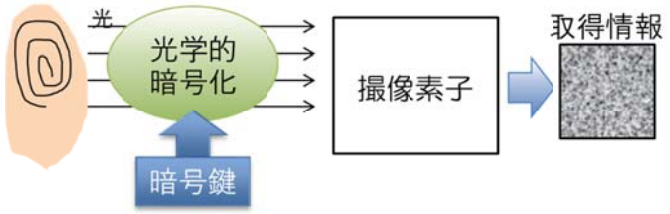


図 3.1 秘匿化センシングの概要



(a)従来のセンシング



(b)秘匿化センシング

図 3.2 従来のセンシングとの比較

秘匿化センシングでは、DRPE とディジタルホログラフィー(DH)を用いる。通常の DH の場合、物体波と参照波である平面波の干渉縞を CCD 等で記録する。本手法では、参照波としてランダム位相変調された光を用いており、この参照波が暗号鍵の役割を果たす。

3.1.1 関連研究

秘匿化センシングに類似した研究例として、Compressed Sensing (CS) に基づく手法[22], [23]とゴーストイメージングに基づく手法[24], [25]を紹介する。

(1) Compressed Sensing (CS) に基づく手法

CS とは、スパース性(零成分が多いという性質)を持つ高次元の信号に対し、少ない観測から再構成を行う信号処理技術である[26], [27], [28]。CS では、センシングの際に、観測行列と呼ばれるものを用いており、再構成を行う際には、観測行列の情報が必要となる。この手法では、観測行列を暗号鍵としてみなし、情報の秘匿化を行っている。文献[23]では、図 3.2 に示すように、静脈からの反射光・透過光を SLM や DMD 等の装置を用いて変調を行い、その強度積分値を取得している。この手法は、秘匿化された状態で情報を計算機内に取り込むため、秘匿化センシングとみなすことができると考えられる。

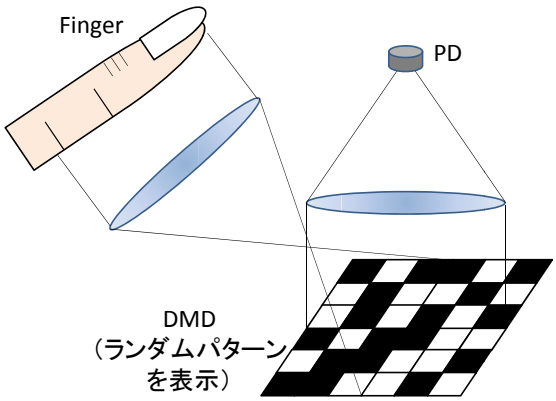


図 3.3　CS を用いた秘匿化センシングでの情報の取得

(2)ゴーストイメージングに基づく手法

ここでは、計算機ゴーストイメージングを用いた手法を説明する。計算機ゴーストイメージングとは、複数回のスペックル照明と点計測と、画像処理技術によりイメージングを行う技術で、リモートセンシング・微弱光イメージング・暗号技術等への応用が期待されている。文献[24]の手法では、光をランダムパターンに通過させることで、スペックル照明を作成し、この照明を物体に照射し、その強度積分値を主としている。ここでは、ランダムパターンを暗号鍵としてみなさている。スペックルパターンによって秘匿化された情報を計算機内に取り込むため、秘匿化センシングとみなすことができると考えられる。

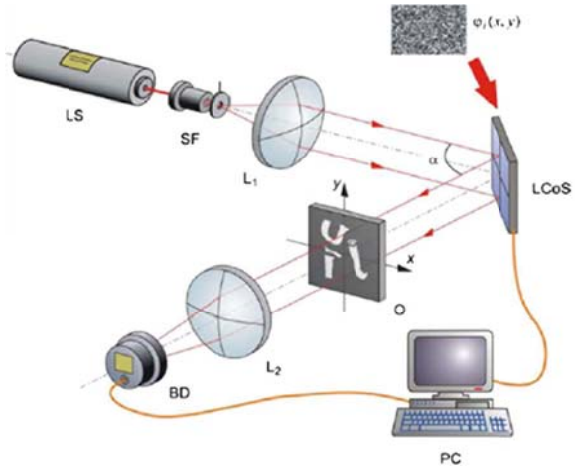


図 3.4　ゴーストイメージングを用いた秘匿化センシングでの情報の取得

3.1.2　ホログラフィーとディジタルホログラフィー

はじめに、ホログラフィーとは、D. Gabor 博士によって提案された，光の波面を記録する技術である[29], [30]。光の色や明るさだけでなく、位相情報も記録できるため、3 次元画像の記録・表示が可能な技術として注目されている。ホログラフィー技術では、波面の振幅情報と位相情報の両方を記録するために、干渉法を用いて強度情報に変換を行う(図 3.5)。物体波$O(x_1, y_1)$と参照波$R(x_1, y_1)$を干渉させ，その干渉縞$I(x_1, y_1)$をホログラムとして撮影する．$I(x_1, y_1)$は以下の式で表される．

$$\begin{aligned} I(x_1, y_1) &= |O(x_1, y_1) + R(x_1, y_1)|^2 \\ &= |O(x_1, y_1)|^2 + |R(x_1, y_1)|^2 + O^*(x_1, y_1)R(x_1, y_1) + O(x_1, y_1)R^*(x_1, y_1) \end{aligned} \tag{3.1}$$

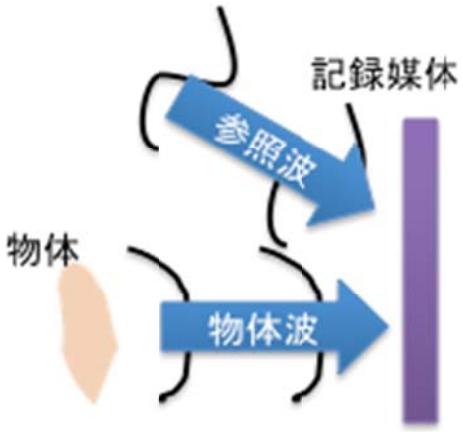


図 3.5 干渉記録

記録した物体波の再生を行う際は、記録の際に用いた参照波$R(x_1, y_1)$かその共役$R^*(x_1, y_1)$で照明する。(3.2)式に参照波で照明した場合の式を示す。

$$\begin{aligned} I(x_1, y_1)R(x_1, y_1) &= R(x_1, y_1)\{|O(x_1, y_1)|^2 + |R(x_1, y_1)|^2\} \\ &\quad + O(x_1, y_1)|R(x_1, y_1)|^2 + O^*(x_1, y_1)R^2(x_1, y_1) \end{aligned} \tag{3.2}$$

この式の第 3 項は物体波に参照波の強度を乗算したものとなる。参照波の強度が一様であると仮定した場合、物体波を複製したものと等しくなる。この際、物体は既に取り去られているにもかかわらず、観測者にはもとの物体から発散してくるように見える。したがって、再生の際の照明として参照波$R(x_1, y_1)$を用いる場合、第 3 項はもとの物体の虚像を発生させていると見なせる(図 3.6)。

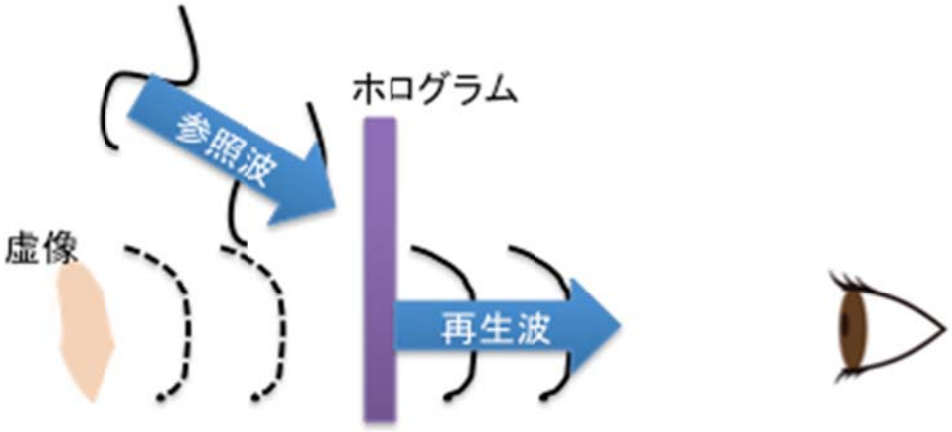


図 3.6 波面再生による結像(虚像)

同様に、参照波の共役$R^*(x_1, y_1)$を照明として用いる場合、(3.3)式に示すような式となる。

$$I(x_1,y_1)R^*(x_1,y_1) = R^*(x_1,y_1)\{|O(x_1,y_1)|^2 + |R(x_1,y_1)|^2\} + O^*(x_1,y_1)|R(x_1,y_1)|^2 + O(x_1,y_1)R^{*2}(x_1,y_1) \tag{3.3}$$

このときの再生波は実像である(図 3.7)。

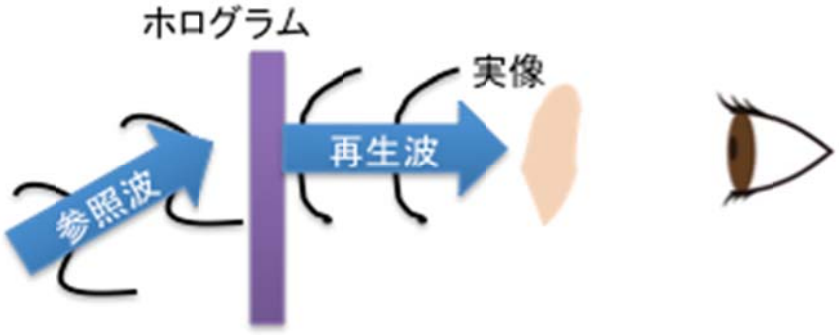


図 3.7 波面再生による結像(実像)

ディジタルホログラフィーは CCD カメラなどの撮像素子を用いて，ホログラフィーの取得を行う技術である．従来のホログラフィー技術との違いとして，事後処理が可能なことや露光時間が短く済むといった利点があるが，CCD の分解能が従来のホログラフィー技術で用いられる感光材に比べて低いため，干渉縞の間隔を CCD の画素ピッチよりも広くしなくてはならないという制約がある．

3.1.3　ディジタルホログラフィーを用いた光学的暗号化手法の実装

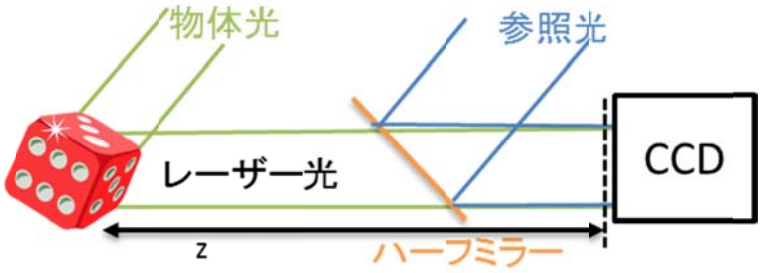
図 3.8(a)は通常の DH の光学系で、得られる干渉縞は以下のように表される。

$$I_a(x_1,y_1)=|FsT[O(x_0,y_0),z]|^2+|R(x_1,y_1)|^2 + FsT[O(x_0,y_0),z]^* R(x_1,y_1)+FsT[O(x_0,y_0),z]R^*(x_1,y_1) \tag{3.4}$$

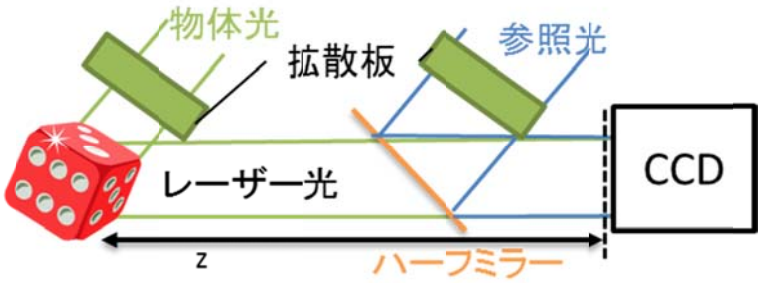
ここで、FsT[]はフレネル伝播のオペレーター、z は伝播距離である。つづいて、図 3.8(b)に示すように、物体波側と参照波側それぞれに拡散板を挿入する。その際の得られる干渉縞は以下のように示される。

$$I_b(x_1,y_1)=|FsT[O(x_0,y_0)\exp\{j\phi_1(x_0,y_0)\},z]|^2+|R(x_1,y_1)|^2 + FsT[O(x_0,y_0)\exp\{j\phi_1(x_0,y_0)\},z]^* R(x_1,y_1) + FsT[O(x_0,y_0)\exp\{j\phi_1(x_0,y_0)\},z]R^*(x_1,y_1) \tag{3.5}$$

この際、$R(x_1,y_1)$はランダム位相変調された光波である。拡散板はそれぞれ、実面とフレネル面での位相変調を行う役割を果たす。フーリエ変換とフレネル変換の違いや$R(x_1,y_1)$が振幅一定でないなどの違いはあるが、(3.4)式の第 3 項(あるいは第 4 項)は(2.2)式で表される DRPE の暗号化画像とみなすことができる。



(a)



(b)

図 3.8 (a)ディジタルホログラフィーの光学系、(b)ディジタルホログラフィーの系を用いた秘匿化センシングの光学系 (D1 と D2 は拡散板)

3.2　秘匿化センシングを用いた生体情報の取得と復元

3.2.1　取得

初めに、生体情報の取得を行う。図 3.9 に示すように、本研究で扱う生体情報は指紋である。3.1.2 項で示したように、取得する秘匿化 DH は(3.5)式のようになる。物体波側にプリズムを設置し、プリズムに指を押し当てることで DH の撮影を行う。また、撮影の際に物体波側の拡散板を少しずつ動かしながら複数の DH を撮影しておく。これは、スペックル[31], [32]によるノイズを低減するためである。スペックルとは、レーザー光が粗物体でランダムに散乱され、各点からの散乱波が観察面の各点で重なり合わさって生じるランダムな干渉現象で、この現象によるノイズをスペックルノイズと呼ぶ。本手法では、スペックルノイズを低減させるために、拡散板を少しずつ動かしながら撮影した DH から再生した指紋画像を足し合わせている。

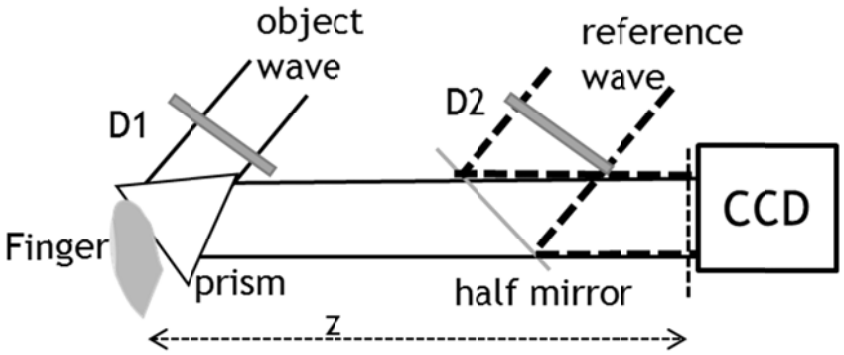


図 3.9 指紋を撮影する際の光学系 (D1 と D2 は拡散版)

本研究では、指紋をモダリティとして用いているが、他の生体情報についても検討を行う。現在、生体認証で用いられる代表的な生体情報は、顔、静脈、虹彩、耳、掌紋、手のひらなどがあげられる。本手法で生体情報を取得する場合は、DH として取得できる必要がある。掌紋は指紋と同様にプリズムに手をおしあてることで、撮影できると考えられる。顔や耳や手のひらなどはそれらに光波を当て、その反射光の DH を撮影すればよい。静脈なども顔などと同様に光波を当て、その反射光を撮影することになる。しかし、静脈は生体内部の情報であるため、光波が生体内に到達するようにする為に、ある程度長い波長(700nm~900nm)である必要がある。さらに、偏光フィルタを用いて、静脈のパターンを効率的に取り出す必要がある。

3.2.2 鍵

秘匿化センシングでは、生体情報を光学的に暗号化し、ディジタル的に復号化を行う。生体情報の再構成を行うために、暗号鍵$K_E(x_1, y_1)$が必要になる。そこで、暗号鍵$K_E(x_1, y_1)$の代わりとして、複素振幅鍵$R_{K_E}(x_1, y_1)$を取得する。その際の光学系を図 3.10 に示し、計算機上で復号鍵を求めるフローを図 3.11 に示す。DH$I_{K_E}(x_1, y_1)$ が複素振幅鍵$R_{K_E}(x_1, y_1)$ と平面波の干渉縞として以下に示すような式として記録される。

$$\begin{aligned} I_{K_E}(x_1, y_1) = & |A_p(x_1, y_1)|^2 + |R_{K_E}(x_1, y_1)|^2 \\ & + A_p(x_1, y_1)^* R_{K_E}(x_1, y_1) + A_p(x_1, y_1) R_{K_E}(x_1, y_1)^* \end{aligned} \tag{3.6}$$

ここで、$A_{K_E}(x_1, y_1)$はexp$\{-j2\pi(ax_1 + by_1\}$で示される平面波で、a と b は$R_{K_E}(x_1, y_1)$と平面波の角度ずれを示すパラメータである。(3.6)式から第 1 項と第 2 項を除去するために、それぞれの光をふさぎながら、強度分布$|R_{K_E}(x_1, y_1)|$と$|A_{K_E}(x_1, y_1)|$を取得しておく。計算機上で(3.6)式から$|R_{K_E}(x_1, y_1)|$と$|A_{K_E}(x_1, y_1)|$を減算し(3.7)式、フーリエ変換を行うことで(3.8)式が得られる。

$$I_{K_E}'(x_1, y_1) = A_p(x_1, y_1)^* R_{K_E}(x_1, y_1) + A_p(x_1, y_1) R_{K_E}(x_1, y_1)^* \tag{3.7}$$

$$i_E'(u_1, v_1) = \delta(u_1 + a, v_1 + b) * r_{K_E}{}^*(-u_1, -v_1) + \delta(u_1 - a, v_1 - b) * r_{K_E}(u_1, v_1) \tag{3.8}$$

ここで、(u_1, v_1)はフーリエ面での座標を示し、$r_{K_E}(u_1, v_1)$は$R_{K_E}(x_1, y_1)$のフーリエ変換である。

a と b が(3.8)式の 2 項を分離できるくらい十分に大きい場合、フィルタリングを行うことで片方だけを得ることができる。フィルタリングしたものを逆フーリエ変換することで、復号化用の複素振幅鍵$R_{K_E}(x_1, y_1)$が得られる(フーリエ変換法[33])。このようにして得られた複素振幅鍵はノイズや再構成の際のエラーなどが考えられるため、オリジナルの暗号鍵$R_{K_E}(x_1, y_1)$と区別して$\hat{R}_{K_E}(x_1, y_1)$とする。

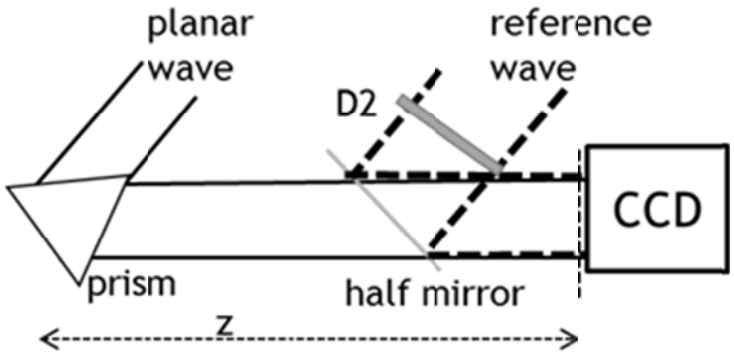


図 3.10 Optical system for obtaining decoding key

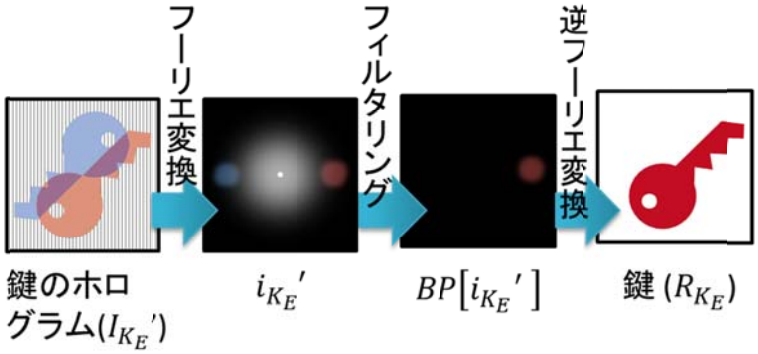


図 3.11 フーリエ変換法による鍵の推定

3.2.3 復元

通常の DRPE((2.3)式)において、復号鍵は振幅一定で位相成分しかもたないとされているが、3.2.2 項で推定した鍵$\hat{R}_{K_E}(x_1, y_1)$は振幅分布を持っている。そこで、波面$D_r(x_1, y_1)$を以下のように再構成する。

$$\begin{aligned} D_r(x_1, y_1) &= C_m(x_1, y_1)\frac{\hat{R}^*_{K_E}(x_1, y_1)}{|\hat{R}_{K_E}(x_1, y_1)|^2} \\ &= FsT[O^*(x_0, y_0)\exp\{-j\varphi_1(x_0, y_0)\}, z]\frac{R_{K_E}(x_1, y_1)\hat{R}^*_{K_E}(x_1, y_1)}{|\hat{R}_{K_E}(x_1, y_1)|^2} \end{aligned} \tag{3.9}$$

これをフレネル伝播させることで、波面$\hat{O}_r(x_1, y_1)$が以下のように得られる。

$$\hat{O}_r(x_2, y_2) = FsT\left[FsT[O^*(x_0, y_0)\exp\{-j\varphi_1(x_0, y_0)\}, z]\frac{R_{K_E}(x_1, y_1)\hat{R}^*_{K_E}(x_1, y_1)}{|\hat{R}_{K_E}(x_1, y_1)|^2}, \hat{z}\right] \tag{3.10}$$

ここで、(x_2, y_2)は復号化の際のフレネル面、$\hat{z}$は復号化の際の伝播距離である。簡単のため、(3.10)式を 1 次元で表わして書き下す。

$$\begin{aligned}\hat{O}_r(x_2) &= A\iint O^*(x)\exp\{-j\varphi_1(x)\}\exp\{-\frac{j\pi}{\lambda z}(x_1-x)^2\}dx \\ &\quad\times \tilde{R}(x_1)\exp\{\frac{j\pi}{\lambda\hat{z}}(x_2-x_1)^2\}dx_1 \\ &= A\int O^*(x)\exp\{-j\varphi_1(x)\}\exp\{-\frac{j\pi}{\lambda}(\frac{x^2}{z}-\frac{x_2^{\,2}}{\hat{z}})\} \\ &\quad\times\int \tilde{R}(x_1)\exp\{\frac{j\pi((z-\hat{z})x_1^{\,2})}{\lambda z\hat{z}}\}\exp\{\frac{-j\pi(2x_1(zx_2-\hat{z}x))}{\lambda z\hat{z}}\}dx_1dx\end{aligned} \tag{3.11}$$

ここで、$\hat{R}(x_1) = R_{K_E}(x_1,y_1)\hat{R}^*_{K_E}(x_1,y_1)/\left|\hat{R}^*_{K_E}(x_1,y_1)\right|^2$、A は比例定数である。式(3.11)内の$x_1$に関する積分の部分を以下のように置く。

$$\beta(x_2'-x) = \int \tilde{R}(x_1)\exp[\frac{j\pi((z-\hat{z})x_1^{\,2})}{\lambda z\hat{z}}]\exp[\frac{-j\pi(2x_1(zx_2-\hat{z}x))}{\lambda z\hat{z}}]dx_1 \tag{3.12}$$

ここで、$x_2' = zx_2/\hat{z}$である。(3.12)式を用いると、(3.11)式を以下のような畳み込み積分で表すことができる。

$$\begin{aligned}\hat{O}_r(x_2) &= A\int O^*(x)\exp[-j\varphi_1(x)]\exp[-\frac{j\pi}{\lambda z}(x^2-\frac{\hat{z}}{z}x_2^{'2})]\beta(x_2'-x)dx \\ &= A\exp[\frac{j\pi\hat{z}}{\lambda z^2}x_2^{'2}](O_{m'}(x_2')*\beta(x_2'))\end{aligned} \tag{3.13}$$

ここで、$O_{m'}(x) = O^*(x)\exp\{-j(\phi_1(x)+\pi x^2/\lambda z)\}$で、*は畳み込み積分の演算子である。$\beta(x_2'-x)$は$\hat{R}_{K_E}(x_1,y_1)$や伝播距離$\hat{z}$に応じて変化する。表 3.1 に$\beta(x_2'-x)$と推定した暗号鍵$\hat{R}_{K_E}(x_1,y_1)$と伝播距離$\hat{z}$の関係を示す。

表 3.1　Values of $\boldsymbol{\beta(x_2'-x)}$.

	$\hat{z}=z$	$\hat{z}\neq z$
$\tilde{R}(x_1)=1$	$A\delta(x_2'-x)$	$A\exp\{-\frac{j\pi\hat{z}(x_2'-x)^2}{\lambda z(z-\hat{z})}\}$
$\tilde{R}(x_1)\neq 1$	$\int \tilde{R}(x_1)\exp\{\frac{-j\pi(2x_1(x_2'-x))}{\lambda z}\}dx_1$	$\int \tilde{R}(x_1)\exp\{\frac{j\pi((z-\hat{z})x_1^{\,2})}{\lambda z\hat{z}}\}\times\exp\{\frac{-j\pi(2x_1(x_2'-x))}{\lambda z}\}dx_1$

$\hat{R}_{K_E}(x_1, y_1)$=1 かつ$\hat{z} = z$である場合、(3.13)式に$\delta(x_2' - x)$を代入すると以下のようになる。

$$\hat{O}(x_2') = AO^*(x_2')\exp\{-j\varphi_1(x_2')\} = O(x_2') \tag{3.14}$$

これより、伝播距離と鍵が適切な場合、生体情報が正しく復元できることがわかる。また、$\hat{R}_{K_E}(x_1, y_1) \approx 1$や$\hat{z} \approx z$であっても、多少ぼけるが、生体情報を復元することが可能である。それ以外の場合では、生体情報を正しく復元することはできない。

$\hat{R}_{K_E}(x_1, y_1) = 1$かつ$\hat{z} \neq z$の場合、(3.13)式に$\exp\{-j\pi\hat{z}(x_2' - x)^2/\lambda z(z - \hat{z})\}$を代入すると以下のように$O^*(x)\exp\{-j\phi_1\}(x)$を距離$z - \hat{z}$でフレネル伝播させたものとなる。

$$\begin{aligned}\hat{O}_r(x_2) &= \exp[\frac{j\pi\hat{z}}{\lambda z^2}x_2'^2](O_{m'}(x_2') * \exp\{-\frac{j\pi\hat{z}(x_2')^2}{\lambda z(z-\hat{z})}\}) \\ &= \int O^*(x)\exp[-j\varphi_1(x)]\exp\{-\frac{j\pi(x-x_2)^2}{\lambda(z-\hat{z})}\}dx\end{aligned} \tag{3.15}$$

$\hat{R}_{K_E}(x_1, y_1) \neq 1$の場合。$\beta(x_2' - x)$はランダム関数列となる。そのため、(3.13)式は生体情報とランダム関数との畳み込み積分で表されるため、生体情報は正しく復元されない。

(3.5)式の第 3 項は厳密には DRPE の暗号化画像とは一致しない。1 点目は、物体波側の拡散板が物体に直接接していない点である。2 点目は、(3.5)式のフレネル面での位相変調が純粋な位相変調にはなっておらず、振幅変調も行われている点である。1 点目の問題については、拡散板から物体までの伝播は 2 つの距離を十分に近づけることで最小化できるため、大きな問題ではない。しかし、2 つ目の問題は十分に考慮する必要がある。図 3.7 に示すように、参照波は拡散板 D2 に変調され CCD センサ面まで伝播するため、CCD センサ面での分布は、D2 による位相変調がフレネル伝播したものと考えられ、これにより発生したスペックルが参照波を変化させている。そのため、正確な再構成を行うためには、R_{K_E}を複素振幅として扱う必要がある。しかし、R_{K_E}の振幅分布の画素値が小さい箇所では、R_{K_E}による除算はエラーを増幅してしまうため、再構成された画像はこのエラーの影響を受けてしまう。この問題を避けるために、R_{K_E}を一様な振幅分布で位相成分のみを持つ波として扱い、式(3.8)を以下のように置き換える。

$$D_r(x_1, y_1) = C_m(x_1, y_1)\frac{\hat{R}^*_{K_E}(x_1, y_1)}{|\hat{R}_{K_E}(x_1, y_1)|} = C_m(x_1, y_1)\exp\{-j\hat{K}_E(x_1, y_1)\} \tag{3.16}$$

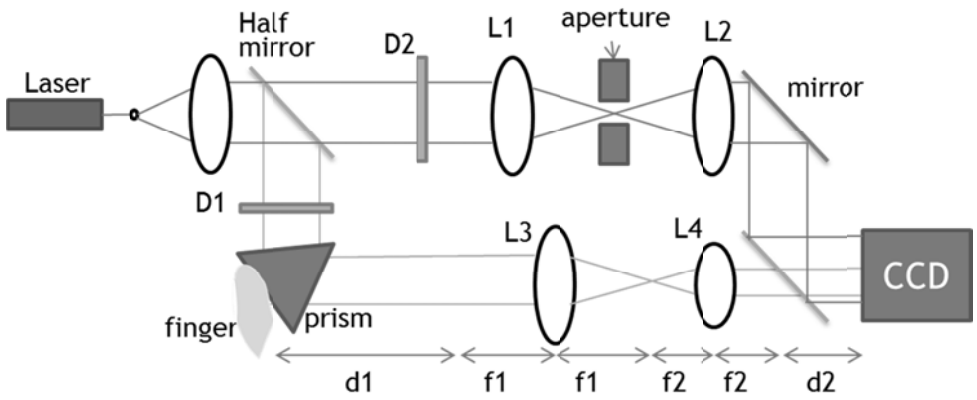
ここで、$\hat{K}_E(x_1, y_1)$は$\hat{R}_{K_E}$の位相成分である。これにより、厳密な計算によって生じてしまうエラーの増幅を抑えることが可能になる。実験では、R_{K_E}の振幅成分が一定かそうでないかの場合について比較を行う。

3.3 実験

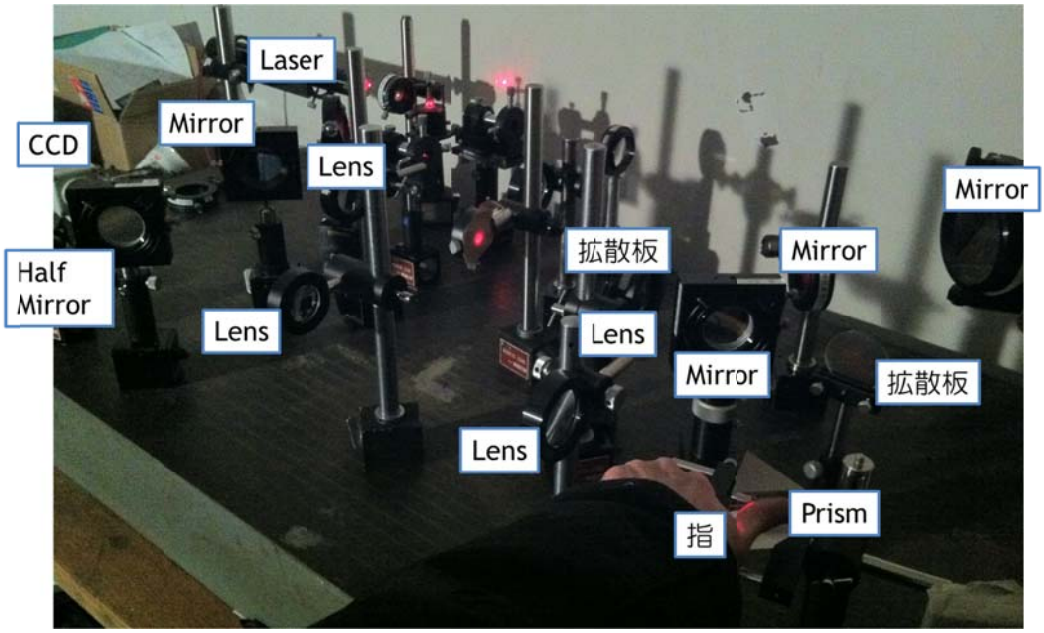
本研究では、暗号化して取得した指紋の DH の再生実験、再生した指紋を用いた照合精度評価実験を行った。

3.3.1 光学系

図 3.12 に実験で用いた光学系を示す。本実験では、波長が 633nm である He-Ne レーザー、画素数が 1024x768[pixel]、画素ピッチが 4.65μm のモノクロ 8 ビット CCD カメラを用いている。各レンズの焦点距離やプリズムから CCD までの距離は図 3.9(a)に併記する。プリズムに指を押し当て、光を照射することで、CCD まで指紋の像を伝播させる。レンズ L3 と L4 を用いて、指紋像の縮小を行っている。



(a)



(b)

図 3.12　実験で用いた光学系の概略(a)と写真(b)

(レンズ L1L2L3 の焦点距離 f1=0.2m、レンズ L4 の焦点距離 f2=0.1m、d1=0.056m、d2=0.2)

3.3.2　生体情報の復元

3.2.3 項で述べたように、復号化画像を 2 つの方法によって計算する。復号鍵である$R_{K_E}(x_1, y_1)$を(3.9)式に示すように複素振幅光波として扱うか、式(3.16)に示すような振幅一定の光波として扱うかの 2 通りである。図 3.13 に暗号化 DH と鍵のホログラム、図 3.14 に復号化画像を示す。暗号化 DH からは指紋を視認できないことが図 3.9(a)より確認できる。

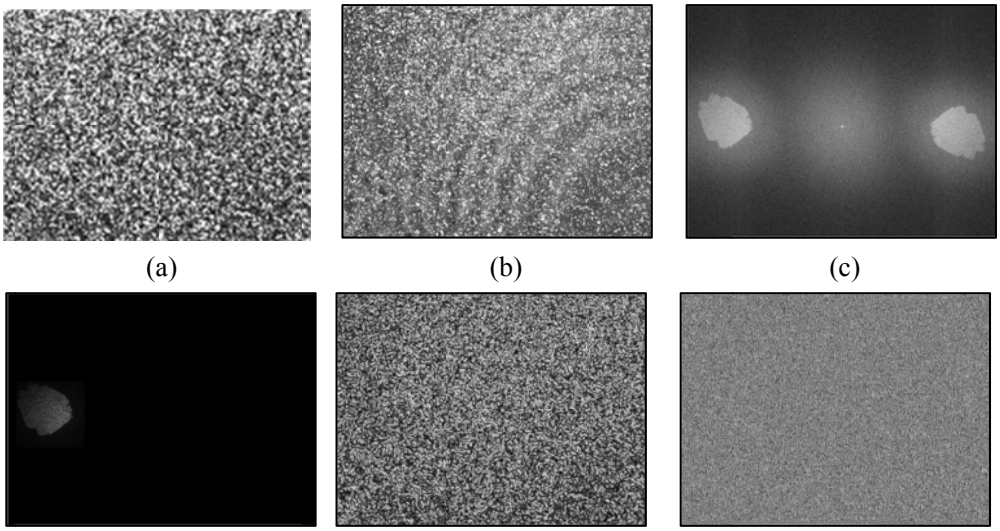
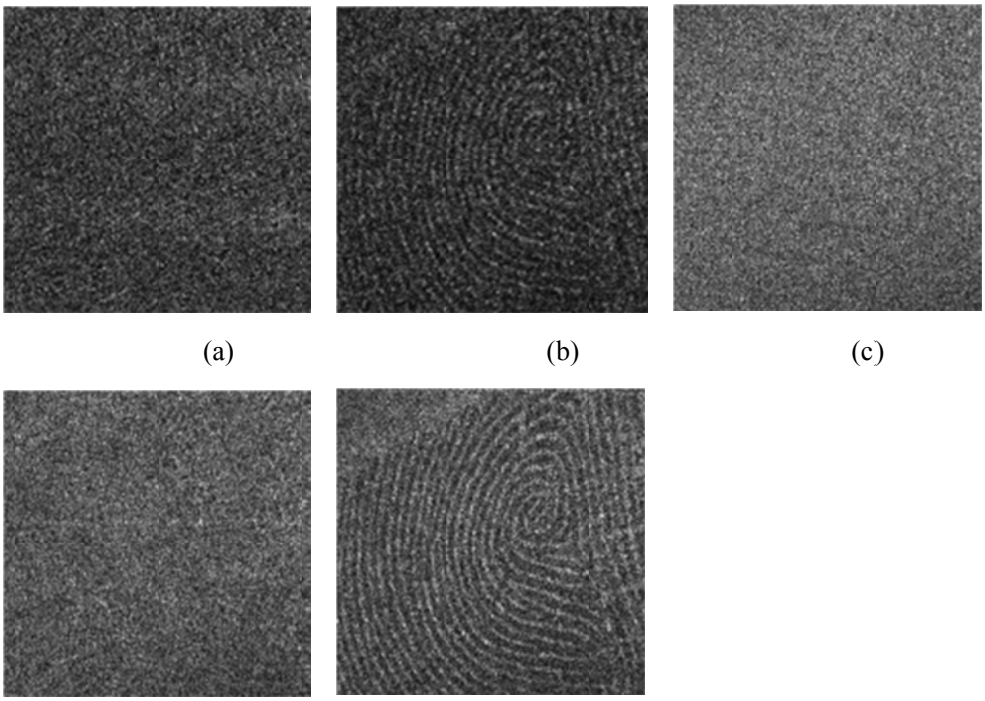


図 3.13 生体情報の復号化 (a): 暗号化ホログラム, (b): 暗号鍵のホログラム, (c): (b)のフーリエ変換, (d): (c)をフィルタリングしたもの, (e): (d)のフーリエ変換の振幅成分, (f): (d)のフーリエ変換の位相成分

図 3.14(a)は復号鍵を複素振幅として扱った場合の復号化画像である。この場合、指紋を識別することは難しい。それに対し、復号鍵を振幅一定化した場合の復号化画像では、指紋をはっきりと確認できる(図 3.14(b))。これより、復号鍵を複素振幅として扱うよりも振幅一定として扱ったほうが、厳密に鍵を複素振幅として扱う場合よりも良い結果を得られることがわかる。図 3.14(c)と(d)には、間違った復号鍵で復号化した場合と、正しい鍵だが間違った伝播距離で復号した場合の復号化画像を示す。どちらの場合においても、ランダムパターンのような画像が得られることが確認できる。

図 3.14(b)の復号化画像は、指紋の形状は確認できるが、まだまだノイズが多いといえる。これは、前述のとおり、スペックルノイズの影響によるものである。図 3.14(e)にはスペックルを低減した画像を示す。図 3.14(b)の復号化画像よりも、より明瞭な指紋画像が確認できる。スペックルの低減は、撮影の際に物体波側の拡散版を移動させながら複数の暗号化 DH を取得しておき、それぞれを復号化したものを足し合わせて行っている(図 3.15)。



(a) (b) (c)

(d) (e)

図 3.14 生体情報の復号化 (a): 復号化した指紋 (複素振幅鍵), (b): 復号化した指紋 (位相鍵), (c): 復号化画像 (間違った鍵), (d): 復号化画像 (正しくない伝播距離 244mm), (e): 復号化した指紋 (スペックル低減)

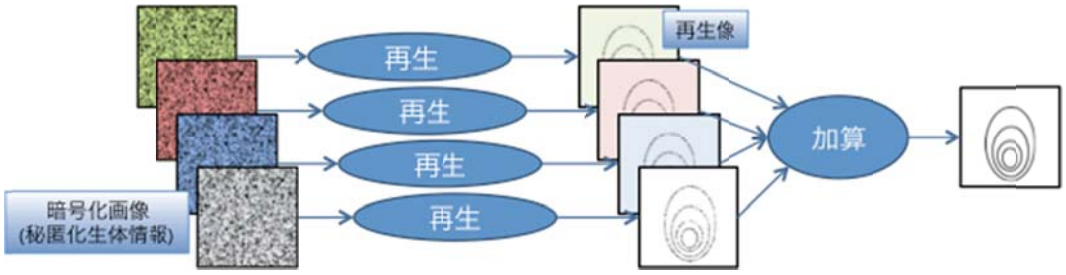


図 3.15 スペックル低減のフロー

3.3.2 復元した生体情報を用いた照合精度評価

取得した DH から復号化した指紋を用いて照合精度評価実験を行った。本実験では、10 人の被験者に対し、それぞれ 10 枚の DH(スペックル低減分を含めると 40 枚の DH)を取得した。照合は 10 枚中の 5 枚を登録用、残りを照合用とし、本人照合を各被験者に対し 25 回、合計で 250 回、他人照合を各被験者に対し 45 回、合計 450 回行った。本照合精度評価

実験では、非線形相関[34]に基づくパターンマッチングを用いて照合を行った。2 つの画像間での非線形相関$c(x,y)$は以下の式で示される。

$$c(x,y) = IFT[|F_1(u,v)F_2(u,v)|^k \exp[j\{\varphi_{F_1}(u,v) - \varphi_{F_2}(u,v)\}]] \qquad (3.17)$$

ここで、$F_m(u,v)$ $(m = 1,2)$は各画像のフーリエ変換を示し、IFT[]は逆フーリエ変換の演算子、$\phi_{F_m}(u,v)$と$F_m(u,v)$の位相分布 k は振幅成分を累乗する指数である(図 3.16)。本実験では、k を 0.3 として実験を行った。これは、k を[0,0.5]の範囲で変化させながら照合を行い、もっともよく識別ができたときの値である。図 3.17 と図 3.18 にスペックル低減を行った場合と行っていない場合の非線形相関の波形を示す。図 3.17(a)、図 3.18(a)より、本人の場合は鋭いピークが生じていることが確認できる。スペックル低減の有無で比較すると低減を行ったほうが、より鋭いピークとなっている。一方で、図 3.17(b)、図 3.18(b)より、他人の場合、ピークは生じていない。図 3.17(c)と図 3.18(c)には本人だが片方は正しい鍵で復号化し、もう片方は異なる鍵で復号したもの(つまり正しく復号化できていない)との非線形相関を示す。たとえ、同じ指紋から得られた DH を復号化したものであっても、鍵が正しくない場合では、ピークが発生しないことが確認できる。

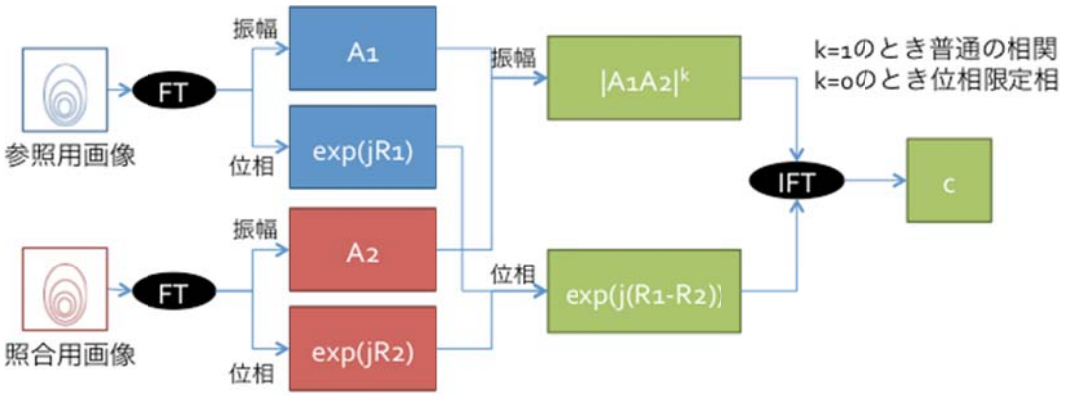
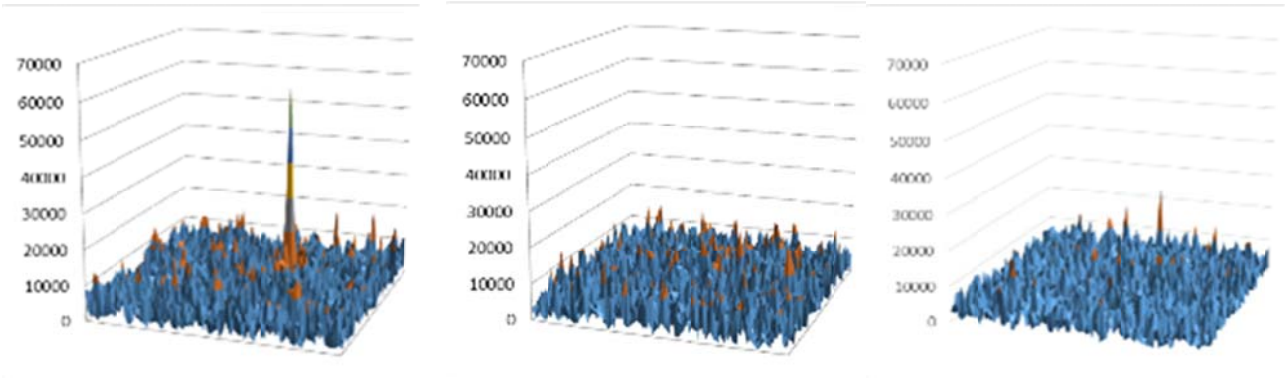


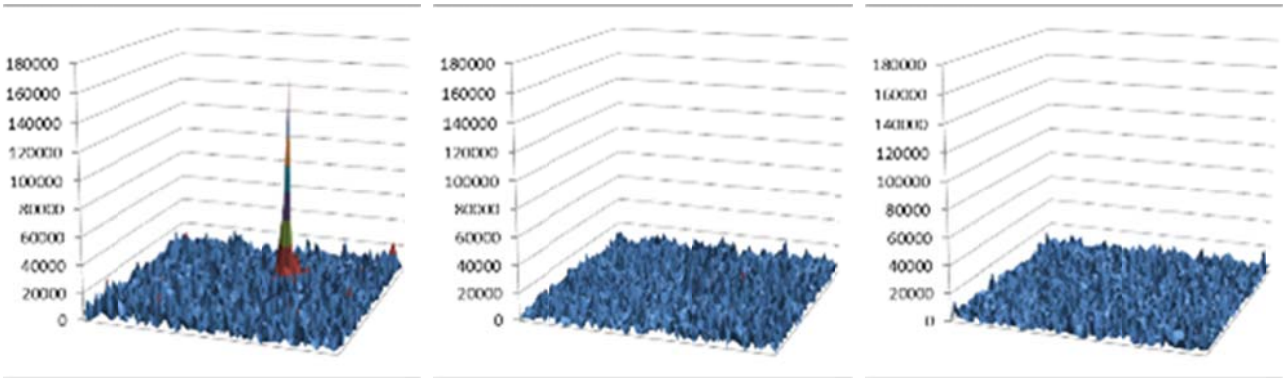
図 3.16　非線形相関



PSR=0.30　　PSR=0.079　　PSR=0.12

(a)　　(b)　　(c)

図 3.17 非線形相関(スペックル低減なし) (a) 本人, (b) 他人 (c) 本人(異なる鍵)



PSR=0.44　　PSR=0.092　　PSR=0.089

(a)　　(b)　　(c)

図 3.18 非線形相関(スペックル低減あり) (a) 本人, (b) 他人 (c) 本人(異なる伝播距離)

照合では、得られた非線形相関から **PSR** を求め、この値を照合の定量的な尺度とする。PSR は以下の式で表される。

$$PSR = \frac{peak - mean}{\sigma} \tag{3.18}$$

ここで、σは非線形相関$c(x,y)$の標準偏差、peak は非線形相関$c(x,y)$のピーク値、mean は非線形相関$c(x,y)$の平均である。PSR の値を用いて、本人排他率(False Rejection Ratio (FRR))と他人受入率(False Acceptance Ratio (FAR))を計算する。図 3.19 に ROC カーブ、図 3.20 に EER(Equal Error Ratio)のグラフを示す。EER は第 2 章と同様の方法で算出している。図 3.19 の ROC カーブはあるしきい値での横軸に FRR、縦軸に FAR をプロットしたものである。この ROC カーブには既存の指紋センサ (U.are.U 4000B、DigitalPersona 社製、8 ビットグレ

ースケール、256×256[pixel]、第２章の自前 DB として用いたもの) で採取した指紋での照合精度評価結果も併記する。スペックル低減を行わない場合の EER が 35.0%であるのに対し、スペックル低減を行った場合の EER が 12.4%となっており、スペックル低減の影響により、照合精度を大きく改善できることが確認できる。

これらの精度は既存の指紋センサで取得した指紋を用いて照合をした場合の精度(EER=0.4%)と比べると決して良いものとは言えない。既存のセンサに比べて精度が悪くなる原因は 3 つあると考えられる。1 つ目は指紋を固定するガイドなどを用いなかったこと、2 つ目は指をプリズムに押し当てる際の強さを特に指示しなかったこと、3 つ目はスペックル低減のための複数の DH を撮影するのに数秒かかってしまっていることである。3 点目に関しては、時間がかかればかかるほど、指が動いてしまう可能性が大きくなってしまう。その場合、足し合わせても、スペックルが低減するどころか、逆に画像がぼけてしまう可能性がある。これらの原因を解消することで、照合精度をさらに改善できると考えている。

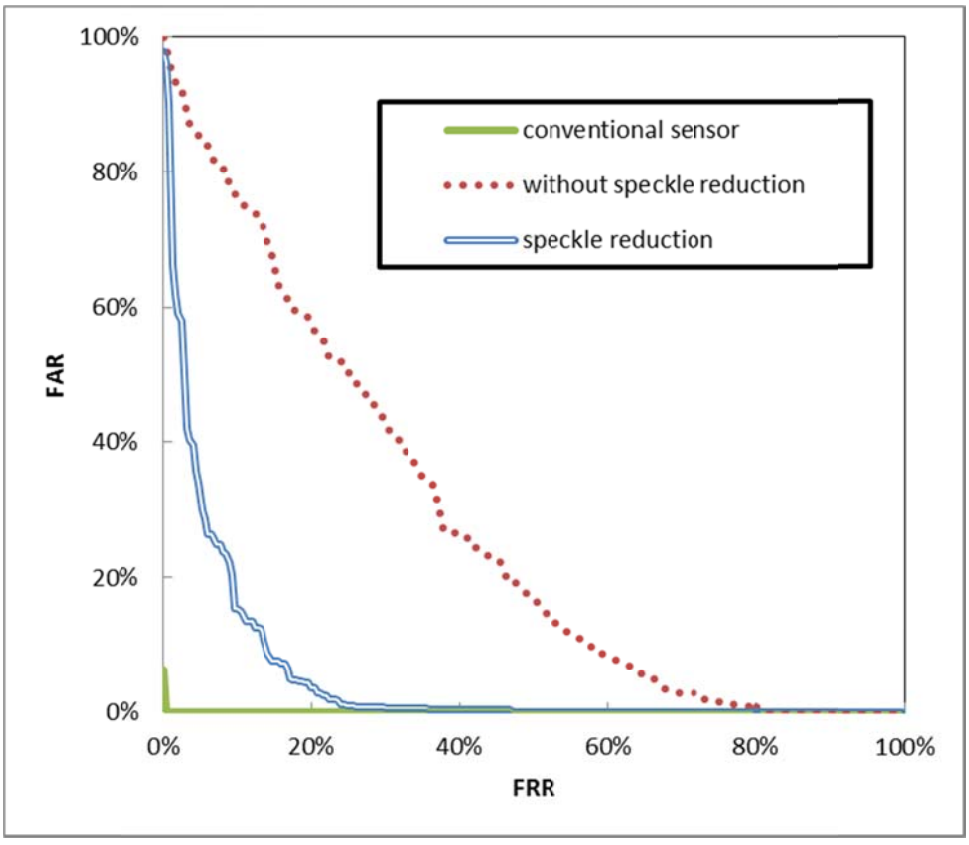


図 3.19　ROC カーブ

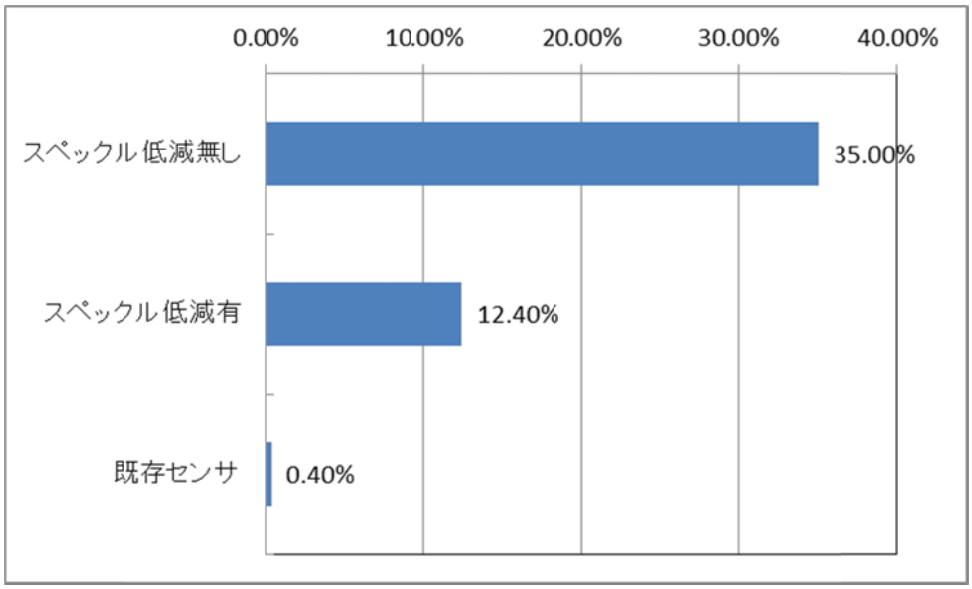


図 3.20 EER のグラフ

3.4　第３章のまとめ

第 3 章では、ディジタルホログラフィーと光学的暗号化手法を用いて生体情報を秘匿化した状態で取得する秘匿化センシングのシステムを提案し、その有効性を実験で確認した。正しい鍵と正しい伝播距離であれば、暗号化 DH から適切に指紋画像を復号化できることを確認した。あらかじめ複数の DH を撮影しておき、スペックル低減した画像を用いて照合精度評価実験をおこない、それなりの精度で照合を行えることとまだまだ改善の余地があることを示した。

本システムの主な利点は生体情報を取得する際に生の指紋をセンシングするのではなく光学的に暗号化した DH を取得することで、安全性を強化することである。これは、光学的な情報は、電子的に保存されている情報よりも漏えいや盗難の危険にさらされることが少ないと考えられるためである。本システムを PUF(Physically unclonable functions)[35], [36], [37]などと組み合わせることで、非常に安全性の高い個人認証システムを開発できると考えられる。

第４章　応用例の検討

第 4 章では、第 2 章で述べた生体情報を鍵とする暗号化手法、第 3 章で述べた光学的暗号化手法を用いた生体情報の秘匿化センシングの応用例についての検討を行う。生体情報を鍵とする暗号化手法をチャレンジアンドレスポンス型認証へ応用した際の利点や欠点について検討を行う。つづいて、秘匿化センシングを用いた生体認証についても検討を行う。最後に、秘匿化センシングを生体認証ではなく、真贋判定・偽造防止へ応用するための検討を行う。

4.1　生体情報を鍵とする光学的暗号化手法を用いた生体認証システム

本研究では、リモート生体認証[38]と呼ばれるインターネット等のオープンなネットワークを介した生体認証について検討を行う。つまり、とある利用者がオープンなネットワークを介してとあるサービスを利用したい際に、自分が正しい利用者であることをサービス提供者に対して証明したい、という状況である。

本論文では、いくつかのシステムに対し、生体情報を鍵とする光学暗号化を適用し検討を行う。

4.1.1　チャレンジアンドレスポンス型認証に適用した場合その 1[39]

図 4.1 と図 4.2 に生体情報を鍵とする暗号化手法をチャレンジアンドレスポンス型認証に適用した際の登録フローを示す。登録は以下のような手順で行う。

1. 秘密鍵を生成
2. 秘密鍵のハッシュを生成
3. 生成したハッシュをサーバに登録
4. 生体情報を提示し、秘密鍵を暗号化し、暗号化画像を生成
5. 生成した暗号化画像を IC カードのなどの持ち運べるデバイスに保存

認証は以下のような手順で行う。

1. IC カードから暗号化画像を提示
2. 生体情報を提示して、秘密鍵を復号化
3. 秘密鍵のハッシュを生成
4. サーバで乱数を生成
5. 登録してあるハッシュを鍵として生成した乱数を暗号化し、チャレンジコードを生成
6. チャレンジコードをクライアントに送信
7. 先ほど復元したハッシュを鍵として、チャレンジコードを復号化し、レスポンスコー

ドを生成

8. サーバにレスポンスコードを送信する
9. 初めに生成した乱数と比較を行う

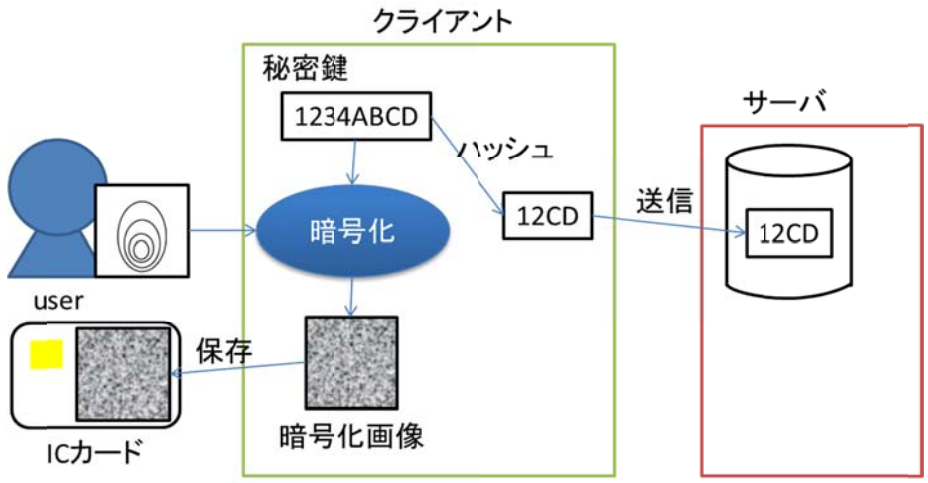


図 4.1　生体情報を鍵とする暗号化手法をチャレンジアンドレスポンス型認証その 1 に適用した際の登録フロー

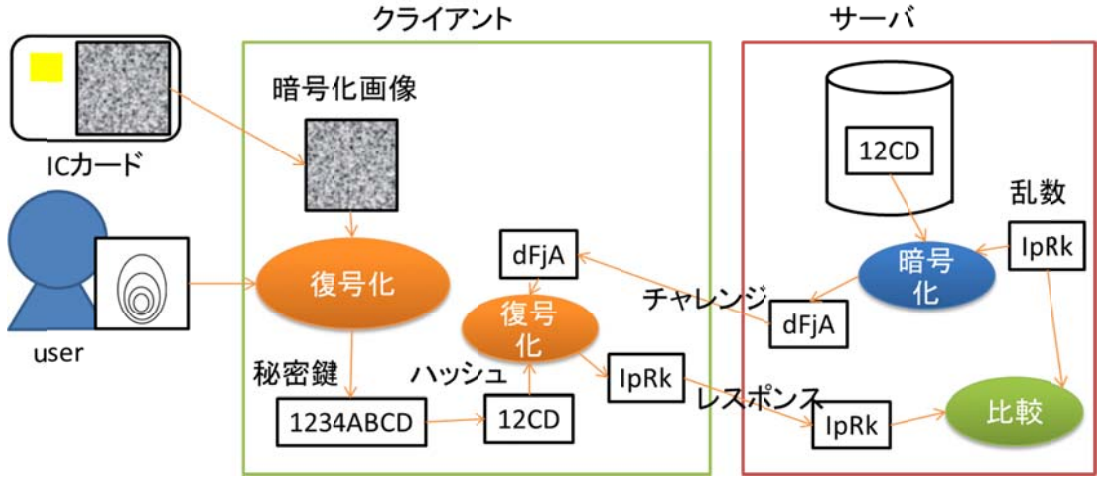


図 4.2　生体情報を鍵とする暗号化手法をチャレンジアンドレスポンス型認証その 1 に適用した際の認証フロー

本システムでは、秘密鍵のハッシュをサーバに登録しているが、公開鍵と秘密鍵のペアを使用し、サーバに公開鍵を登録しても同様にチャレンジアンドレスポンス認証を行うこ

とが可能である。

本システムにおいて、通信路を流れる情報はチャレンジとレスポンスである。登録してあるハッシュや生体情報は通信路には流れない。通信路からの情報漏えいに関しては、既存のチャレンジアンドレスポンス型認証と差異はなく、リプレイ攻撃にも耐性を持つ。

ユーザは認証時にクライアント端末に対し、生体情報と暗号化画像を提示する必要があり、通常時はクライアント端末内に生体情報や暗号化画像は存在しない。そのため、クライアント端末への攻撃への耐性は高い。

サーバに登録する情報は秘密鍵のハッシュであり、生体情報とは一切関連のない情報であるため、サーバに対して生体情報を秘匿することができている。しかし、逆に言えば、ユーザが本当に適切な生体情報を所有しているかを直接確認することができない。登録してあるハッシュが漏えいなどの何らかの理由でばれてしまった場合は生体情報を持たずとも認証することができてしまう。万が一、サーバに登録したハッシュの情報が漏えいしてしまった場合、すぐに登録情報の更新を行う必要がある。しかし、登録する情報は生体情報とは一切関連のない情報であるため、何度でも再登録が可能であり、キャンセラブル性は高いといえる。

4.1.2 チャレンジアンドレスポンス型認証に適用した場合その 2[40]

図 4.3 と図 4.4 に生体情報を鍵とする暗号化手法をチャレンジアンドレスポンス型認証に適用した際の登録フローを示す。登録は以下のような手順で行う。

1. 乱数を生成
2. 生体情報を提示して、乱数を暗号化
3. 生成した暗号化画像をサーバに登録
4. 乱数を IC カードのなどの持ち運べるデバイスに保存

認証は以下のような手順で行う。

1. IC カードから乱数を提示
2. 生体情報を提示して、乱数を暗号化
3. サーバで乱数を生成
4. 登録してある暗号化画像を鍵として、生成した乱数を暗号化し、チャレンジコードを生成
5. チャレンジコードをクライアントに送信
6. 先ほど生成した暗号化画像を鍵として、チャレンジコードを復号化して、レスポンスコードを生成
7. サーバにレスポンスコードを送信
8. 3 においてサーバで生成した乱数とレスポンスコードの比較を行う

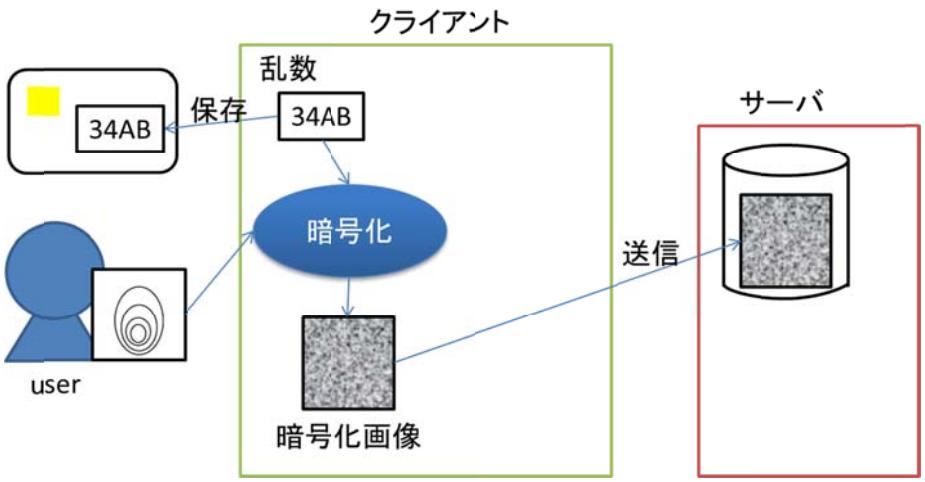


図 4.3　生体情報を鍵とする暗号化手法をチャレンジアンドレスポンス型認証その 2 に適用した際の登録フロー

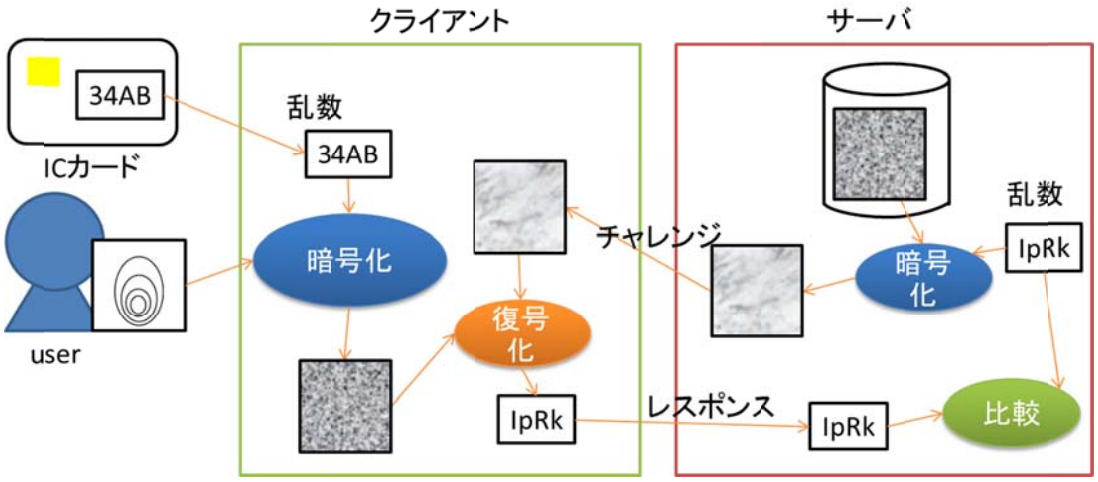


図 4.4　生体情報を鍵とする暗号化手法をチャレンジアンドレスポンス型認証その 2 に適用した際の認証フロー

本システムにおいて、通信路を流れる情報はその 1 と同様、チャレンジとレスポンスであり、登録してあるハッシュや生体情報は通信路には流れない。しかし、チャレンジは画像であるため、その 1 と比べると通信の負荷は大きくなる可能性がある。

ユーザは認証時にクライアント端末に対し、生体情報と登録時に用いた乱数を提示する必要がある。ここでもその 1 と同様、通常時はクライアント端末内に生体情報や暗号化画像は存在しない。しかし、提示する情報はその 1 とは異なり暗号化画像ではなく、乱数で

あるため、実用的に記憶可能な長さであれば、IC カードを用いずにパスワードとして記憶することも可能である。

本システムでは、暗号化画像をサーバに登録している。そのため、ユーザが本当に適切な生体情報を所有しているかを直接確認することができるといえる。しかし、サーバに対して生体情報を保護するためには、暗号化画像から生体情報を復元することはできない等の一方向性が必要となる。万が一、サーバに登録した暗号化画像が漏えいしてしまって登録をし直す際は、新しく登録する暗号化情報が漏えいしてしまった暗号化画像と無相関であることが求められる。これより、その 1 と比較すると、キャンセラブル性は劣っている可能性がある。

4.2　生体情報の秘匿化センシングの生体認証システムへの応用

秘匿化センシングでは、生体情報を秘匿化した状態で取得することが可能である。鍵を使わない限り取得した情報からは生体情報を復元できず、電子データとして保存しておくことが可能である。秘匿化センシングを生体認証へ応用する場合、生体情報を取り込む際に用いられる。生体情報を復元して使用する際は、耐タンパ性を持つなどのセキュリティの高い装置内で復号化を行わなくてはならない。

図 4.5 と図 4.6 に登録と照合の一例を示す。

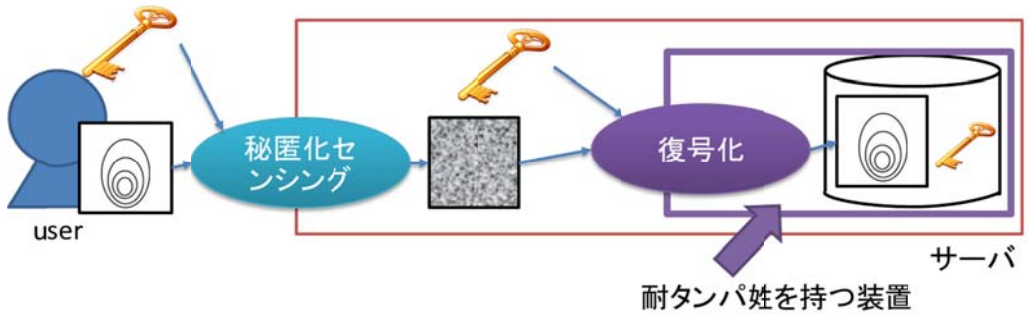


図 4.5　秘匿化センシングを用いた生体認証の登録フロー

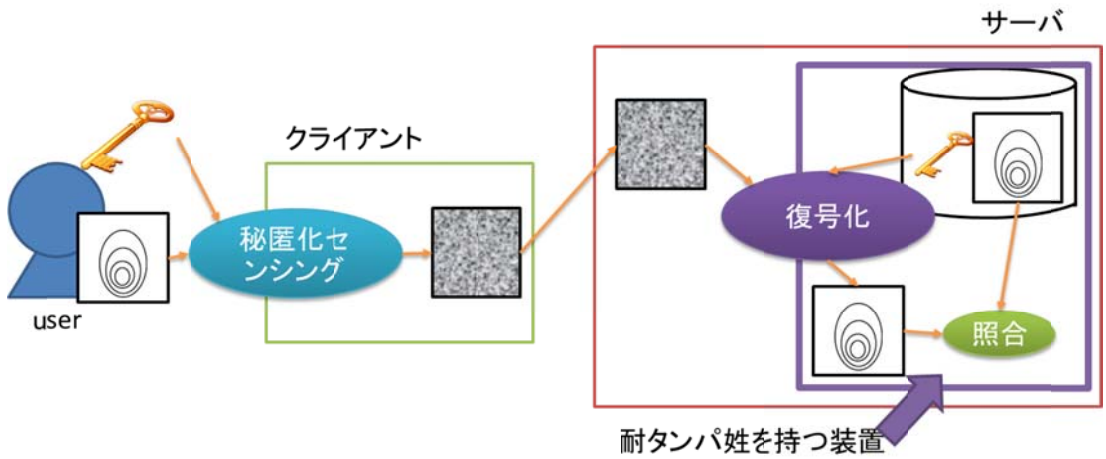


図 4.6　秘匿化センシングを用いた生体認証の認証フロー

登録の際は、ユーザとサーバは直接オフラインで接続しているとし、以下の手順で登録を行う。

1. ユーザは秘匿化センシングを用いて、サーバに暗号化した生体情報を提示する。
2. 鍵(拡散板)はユーザで保管し、データ化した鍵はデータベースに登録する。
3. サーバ内には耐タンパ性を持つ装置があり、その中で生体情報を復号化する。
4. 復号化した生体情報をデータベースに登録する。

認証の際は、ユーザとサーバはクライアントを経てオンラインでつながっているとし、以下の手順で登録を行う。

1. ユーザはクライアント側で生体情報を秘匿化し、秘匿化した生体情報をサーバに送信する。
2. 耐タンパ性を持つ装置内で、サーバに登録してある鍵と送られてきた秘匿化した生体情報を用いて、生体情報を復号化する。
3. サーバに登録してある生体情報と復号化した生体情報を照合する。

本システムでは、登録の際、サーバに直接登録を行う。これは、登録の際に鍵も同時に登録するためである。登録をオンラインで行う場合、鍵と秘匿化した生体情報を送らなくてはならず、2 つセットで盗聴されると、生体情報を盗まれてしまうため絵ある。また、サーバ内には耐タンパ性をもつ装置があると仮定し、その中のデータベースに生体情報を登録する。対タンパ性をもつ装置内のデータベースに生体情報を保管しているため、外部に漏えいしてしまうことは少ない。しかし、サーバに対しては、まったく秘匿化されておらず、プライバシの保護はなされていない。そのため、本システムを運用する場合は、サーバは悪事をたくらむことはないという前提でなくてはならない。この前提が必要である点

を除けば、生体情報は耐タンパ性を有する装置の外では、完全に秘匿化されており、大変安全な生体認証を行うことができると考えられる。

前述のチャレンジアンドレスポンスを用いたシステムでは、登録情報が漏えいしてしまった際は再登録を行うことが可能であったが、本システムは生体情報を登録してあるため、絶対に漏えいしてはならない。

以上のように、本システムは安全ではあるが、制約が多い。そこで、秘匿化センシングを先述のチャレンジアンドレスポンスの手法に応用する。

4.3 秘匿化センシングの真贋判定への応用

本節では、秘匿化センシングを偽造防止や真贋判定などへの適用の可能性について検討を行う。

近年、高級ブランド品やクレジットカード、身分証明書などの偽造による被害・犯罪が増えており、多くの企業から様々な偽造防止技術が提案されている。その一部の例を表 4.2 に示す。１～４の技術はホログラムに基づく技術で、”一目で見分けがつく”、”専用のビューワで判定する”といった具合に真贋判定を行う。５・６は特殊なインクを用いたもので、印刷技術と融合したりや糸に染み込ませたりして用いる。７は新しい画像形成技術よるもので、８は PUF を応用した IC タグである。どの技術も”複製が困難”や” 真贋判定を行うことが可能”といった特徴を持つ。

１～７の技術はタグのようなものを製品に取り付け、専用のカメラなどで撮影・センシングを行うことで、真贋判定を行っている。つまり、同一のロットでは、同じタグが吹かされている。８の SMARTICS-V では、IC タグの回路の微妙な違いによる PUF を用いて、真贋判定を行っている。つまり、各製品によって、タグ(と呼んでおく)は異なることになる。

近年では、偽造が困難といわれていたホログラムも、複製技術の進歩により偽造されているという報告がある[41]。同一のロット内で同じタグを使用するケースの場合、偽造されたタグが貼り付けられたものがまぎれていても気付かない恐れがある。それに対し、各製品によってタグが異なるのであれば、2 つとして同じタグは存在しないため、精巧に偽造できたとしても、重複した場合は偽造だとばれてしまう。

秘匿化センシングでは、製品の粗面にレーザーを当て、散乱光をセンシングすることで、PUF と同等な機能を有することができると考えられる。粗面を反射した光は、ランダムに干渉しあい、スペックルパターンを形成するためである。この際、暗号鍵がなくても十分 PUF と同等のことができると考えられる。

さらに、秘匿化センシングでは、１～７のようなタイプの真贋判定にも対応できると考えられる。秘匿化された CGH を作成、これからホログラムのハードコピーを生成し、タグとする。秘匿化された CGH を作成した際の鍵も作成しておき、これまでの逆で、秘匿化され

たホログラムを作成した鍵を用いてセンシングを行うことで、秘匿化されていない CGH を取り込み、真贋判定を行うことができるようになると考えられる。

以上より、秘匿化センシングを用いることで、どちらのタイプの偽造防止・真贋判定にも対応できることがわかる。

ここで、秘匿化センシングの真贋判定への応用例を示す．多くの場合、真贋判定を行うためには、対象物に対し、タグなどを付加する必要がある．しかし、美術品や芸術品などにタグを付加することは、対象物の景観を破壊してしまう恐れがあるため、タグを付加することはあまり望ましくない．そこで、以下の方法で真贋判定を行うことを考える．登録の際は、対象物の写真あるいは全景を暗号化される平文とする．暗号鍵は対象物の祖面の一部を用いる．これらを用いて秘匿化センシングで撮影を行い、暗号化ホログラムを生成し、サーバなどに登録を行う．暗号化ホログラムは ID などとひもづけて登録しておく．判定を行う際は、はじめに対象物の祖面の DH を撮影し、復号鍵を生成する．次に、サーバから暗号化ホログラムをダウンロードし、先ほど復元した復号鍵を用いて、暗号化ホログラムを複合化する．登録の際に撮影した対象物の全景と同じ物が復号化されれば、対象物は本物であると判定される．これにより、本物にそっくりで素人の目では見分けがつかないような対象物であったとしても、あらかじめ登録をしておけば、タグなどを付加することなく、対象物が本物かどうかの判定を行うことができる。

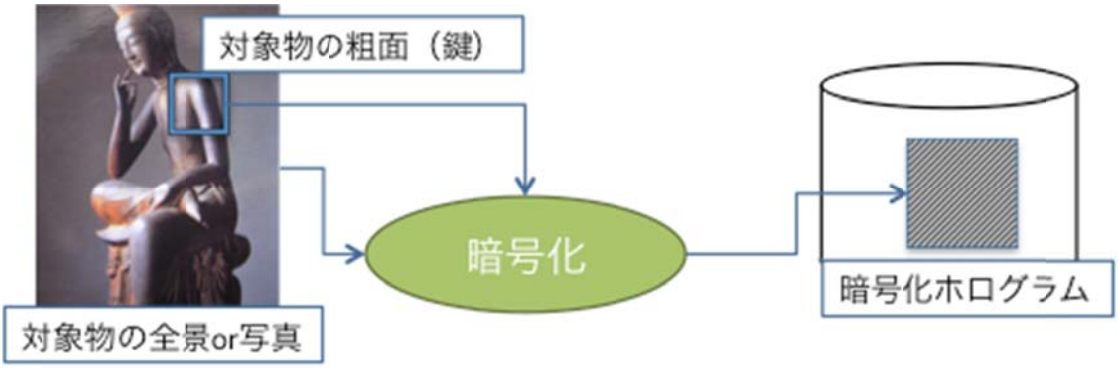


図 4.7　真贋判定の登録

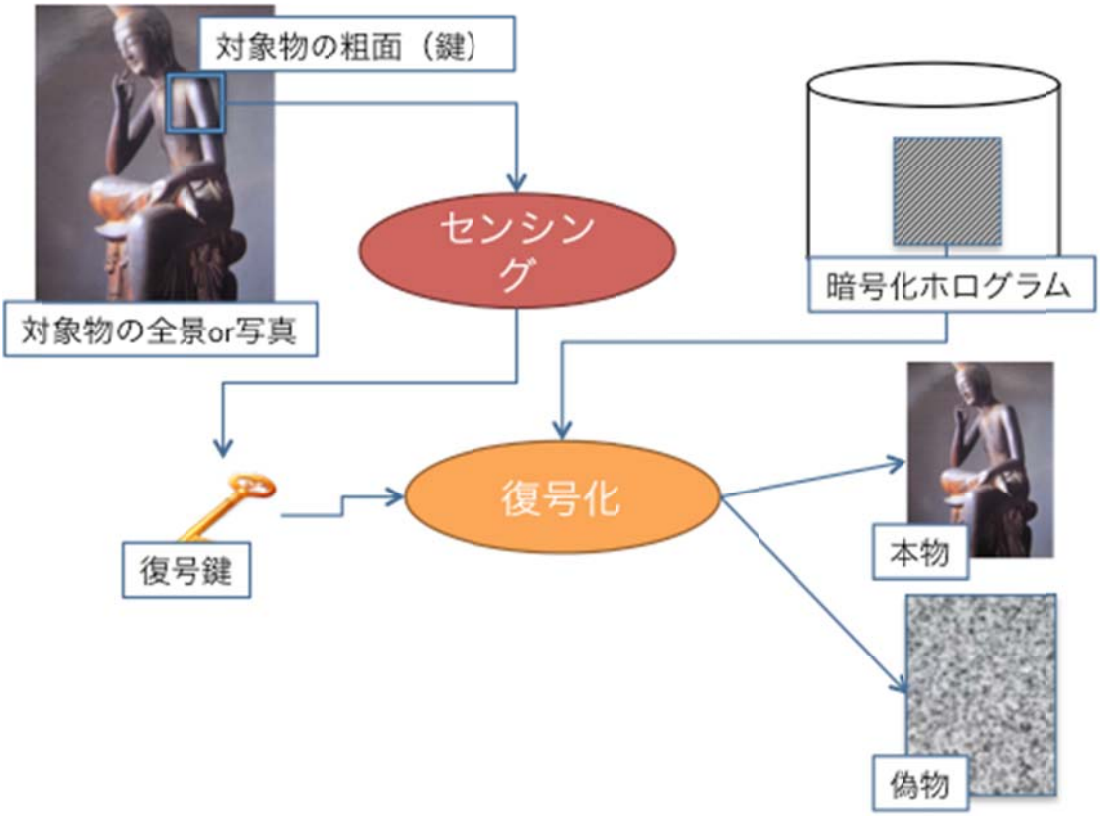


図 4.8　真贋判定の判定

表 4.2　偽造防止・真贋判定技術の例

1　トラストグラム[42]	特殊な光学特性を持つ素材にホログラムを記録した偽造防止デバイス。カラーシフト機能、簡易ビューワによる真贋判定を有する。
2　バーチャグラム[43]	高解像度立体表現により、一目で真贋判定が可能。特殊な光学特性を持つ材料をホログラム上に印刷することで、専用のビューワによる真贋判定も可能。
3　モーションイマージュ[44]	立体感に優れるリップマンホログラムを採用し、上下左右に視点を移動させたときに、3 次元画像がアニメーションのように動いて見え、一目で偽造品との見分けがつく。通常のリップマンホログラムよりもさらに高度な技術とノウハウを必要とし偽造が困難。
4　パールグラム[45]	光の回折だけでなく、散乱・吸収など多くの光学的要素を考慮した新次元の光学デバイス。
5　アルタテックス[46]	特殊な光学特性を持つインクを使用した偽造防止デバイス。ブランドラベルとして、繊維製品に直接縫い付けて使用可能。
6　DNA インキ[47]	植物由来の DNA を用いたセキュリティ技術。多様な印刷技術と組み合わせることで、高いセキュリティ機能を持つ偽造防止製品の提供が可能。
7　フォージガード[48]	全く新しい画像形成法により、ラベルをカラー化。高い偽造難易度と高い表現力を有する。専用ビューワをかざすだけで真贋判定が可能。
8　SMARTICS-V[49]	PUF 技術[35], [36], [37]を搭載した IC タグ。NFC に対応した IC タグを使用し、データベースと照合することで真贋判定を行うことが可能。

4.4　第 4 章のまとめ

第 4 章では、生体情報を鍵とする暗号化手法や秘匿化センシングをどのように生体認証に応用していくかを検討し、さらに秘匿化センシングの偽造防止・真贋判定への応用の可能性についても検討した。

生体情報を鍵とする暗号化手法を用いた生体認証として、チャレンジアンドレスポンスに基づく手法を 2 つ検討した。サーバに登録する情報を何にするかに応じて、安全性や利

便性が変わることを示した。

秘匿化センシングの生体認証への応用では、サーバ側に耐タンパ性を持つ装置を仮定した認証システムを検討した。多くの制約があるが、安全に生体認証を行うことができる可能性を示した。

秘匿化センシングの偽造防止・真贋判定への応用では、既存の偽造防止・真贋判定技術との比較を行い、秘匿化センシングを応用した場合の特徴を検討した。

第５章　結論

本論文では、光学的暗号化手法を応用した生体認証として、生体情報を鍵とする暗号化手法の問題点の改善や生体情報の秘匿化センシングについて検討を行った。

生体情報を鍵とする光学的暗号化手法には他人の生体情報での復号化画像に平文画像のシルエットがぼんやりと映ってしまっている問題や回転補正時に行うタグ画像との相関演算が攻撃者の手掛かりになっている恐れがある問題などが存在する。第 2 章では、これらを解決するために、平文画像や鍵画像の生成手法を検討した。はじめに、平文画像の改善として、従来の平文画像であるビットパターン画像のフーリエ変換ホログラムを新たに平文画像として採用した。ビットパターン画像はランダム位相変調を施されたのちにフーリエ変換されるため、生成されるホログラムは空間分布の偏りがない画像となり、シルエットがぼんやり映ってしまうこともなくなった。さらに、ホログラム平文画像を用いることで、生体情報に位置ずれが生じている場合でも、復号化されるビットパターン画像には位置ずれは生じないという特徴もある。指紋の揺らぎに対するロバスト性を向上させるために、得られたホログラムを 2 値化した。また、フーリエ反復を用いて 2 値化の際の誤差が最小になるように最適化されている。つづいて、タグ画像との相関演算を行わなくても復号化できるようにするために、鍵画像の改善として、回転不変暗号鍵を用いた。回転不変暗号鍵は少しずつ回転させた生体情報の画像から生成した鍵を学習データとし、フィルタ設計を応用して作成する。回転不変暗号鍵を用いた場合でも十分な相関ピークが得られることも確認している。また、復号化の際に、回転補正を行わないため、復号化にかかる時間を短縮できる利点も有する。実験では、ホログラム平文画像や回転不変暗号鍵を採用した際の照合精度評価実験を行い、ホログラム平文画像を採用しても十分に精度を維持しながら復号化を行え、他人の生体情報での復号化画像に平文画像のシルエットが写っていないこと、回転不変暗号鍵を採用しても十分な精度を維持できていることを確認した。また、ホログラム平文画像の生体情報の誤差に対するロバスト性や他人の生体情報での復号化画像のランダム性を調査し、従来手法ほどではないが十分なロバスト性を有することと他人の生体情報での復号化画像のランダム性が十分に高いことを確認した。

第 3 章では、ディジタルホログラフィーの系を応用して光学的暗号化手法を光学実装し、生体情報を秘匿化した状態で取得する秘匿化センシングを提案した。生体情報は重大な個人情報であり、漏洩した場合取り返しがつかなくなってしまうため、厳重に保護されなくてはならない。既存のセンサでは、取得した生体情報は電子データとして存在するため、漏洩の危険性をはらんでいるのに対し、秘匿化センシングでは、センシングした段階で生体情報が秘匿化されているため、生体情報が漏洩してしまう危険性は低くなる。本論文では、光学系を構築して秘匿化した状態で生体情報を取得し、計算機条で復号化して照合を行うことができることを確認した。

第 4 章では、生体情報を鍵とする光学的暗号化手法や秘匿化センシングの生体認証への適用について検討を行った。チャレンジアンドレスポンスを用いた手法などについて検討を行い、安全に生体認証を行うことができる可能性を示した。

本論文では、光学的暗号化手法を応用することで、生体認証をより安全に行うことができる可能性を示した。照合精度などの面では、既存の手法に比べ、劣る部分もある。しかし、生体情報の揺らぎを吸収できる点や光の段階で暗号化を行うことができる点など、既存の手法にはない特徴を有し、生体認証のさらなる発展に寄与できると考えられる。今後の課題として、既存手法と同程度の精度・計算時間を得ることや装置の光学系の小型化などが挙げられる。

付録

1. MACE フィルタ[15]

$\mathbf{D}$ は正則行列である。$\mathbf{h}^{+}\mathbf{Dh}$ を最小化し、以下の拘束条件を満たす解 $\mathbf{h}$ を求める。

$$\mathbf{X}^{*}\mathbf{h} = \mathbf{u} \tag{6.1}$$

式(6.1) の拘束条件より、以下の関数が極値にあると表現されるため、この関数を最小にする時の $\mathbf{h}$ を求めればよい。

$$\phi = \mathbf{h}^{*}\mathbf{Dh} - 2\lambda_1(\mathbf{h}^{*}\mathbf{x}_1 - u_1) - \ldots - 2\lambda_M(\mathbf{h}^{*}\mathbf{x}_M - u_M) \tag{6.2}$$

ここで、$\lambda_1,..,\lambda_N$ は未定乗数、$\mathbf{x}_i$ は行列 $\mathbf{X}$ の i 番目の列ベクトル、u_i は列ベクトル $\mathbf{u}$ の i 番目の要素である。この式を $\mathbf{h}$ で微分すると以下のような式が得られる。

$$\mathbf{Dh} = \lambda_1\mathbf{x}_1 + \ldots + \lambda_M\mathbf{x}_M \tag{6.3}$$

$\mathbf{D}$ は正則行列であるので、$\mathbf{h}$ は以下のように表わされる。

$$\mathbf{h} = \mathbf{D}^{-1}\sum_{i=1}^{M}\lambda_i\mathbf{x}_i = \sum_{i=1}^{M}\lambda_i\mathbf{D}^{-1}\mathbf{x}_i \tag{6.4}$$

ここで、$\mathbf{l} = [\lambda_1, \lambda_2, .. \lambda_M]$ とすると、

$$\mathbf{h} = \mathbf{D}^{-1}\mathbf{Xl} \tag{6.5}$$

となる。この式を拘束条件の式(6.1) に代入すると、

$$\mathbf{X}^{*}\mathbf{D}^{-1}\mathbf{Xl} = \mathbf{u}$$

$$\mathbf{l} = (\mathbf{X}^{*}\mathbf{D}^{-1}\mathbf{X})^{-1}\mathbf{u} \tag{6.6}$$

となる。この式を式(6.5) に代入すると、

$$\mathbf{h} = \mathbf{D}^{-1}\mathbf{X}(\mathbf{X}^{*}\mathbf{D}^{-1}\mathbf{X})\mathbf{u} \tag{6.7}$$

が得られる。

2. MACH フィルタ[16]

ASM と ONV と ACH を以下のように定義し、ASM と ONV が小さく、ACH が大きくな

るようなフィルタ $\mathbf{h}$ を設計する。

$$\begin{aligned}\mathrm{ASM} &= \frac{1}{Md}\sum_{i=1}^{M}\left|\mathbf{X}_i{}^{*}\mathbf{h}-\mathbf{M}^{*}\mathbf{h}\right|^2 \\ &= \frac{1}{Md}\sum_{i=1}^{M}\mathbf{h}^{*}(\mathbf{X}_i-\mathbf{M})(\mathbf{X}_i-\mathbf{M})^{*}\mathbf{h} \\ &= \mathbf{h}^{*}\left[\frac{1}{Md}\sum_{i=1}^{M}(\mathbf{X}_i-\mathbf{M})(\mathbf{X}_i-\mathbf{M})^{*}\right]\mathbf{h} \\ &= \mathbf{h}^{*}\mathbf{S}\mathbf{h}\end{aligned} \tag{6.8}$$

$$\mathbf{S}=\frac{1}{Md}\sum_{i=1}^{M}(\mathbf{X}_i-\mathbf{M})(\mathbf{X}_i-\mathbf{M})^{*}$$

$$\mathrm{ONV} = \mathbf{h}^{*}\mathbf{C}\mathbf{h} \tag{6.9}$$

$$\mathrm{ACH}=\frac{1}{M}\sum_{i=1}^{M}\mathbf{x}^{*}\mathbf{h}=\mathbf{m}^{*}\mathbf{h} \tag{6.10}$$

ここで、d は画素数、$\mathbf{X}_i$ は列ベクトル $\mathbf{x}_i$ を対角行列に直したものである。また、$\mathbf{m}=\sum_{i=1}^{M}\mathbf{x}_i$ としたとき、$\mathbf{M}$ も同様に列ベクトル $\mathbf{m}$ を対角行列に直したもの、$\mathbf{C}$ はノイズのパワースペクトルを要素として持つ対角行列である。

ASM と ONV を小さくなるようにし、ACH が大きくなるようにフィルタを設計するために、以下のような式を定義し、これが最大になるようなフィルタ $\mathbf{h}$ を求める。

$$\begin{aligned}J(\mathbf{h}) &= \frac{\left|\mathrm{ACH}\right|^2}{\mathrm{ASM}+\mathrm{ONV}} = \frac{\left|\mathbf{m}^{*}\mathbf{h}\right|^2}{\mathbf{h}^{*}\mathbf{S}\mathbf{h}+\mathbf{h}^{*}\mathbf{C}\mathbf{h}} \\ &= \frac{\mathbf{h}^{*}\mathbf{m}\mathbf{m}^{*}\mathbf{h}}{\mathbf{h}^{*}(\mathbf{S}+\mathbf{C})\mathbf{h}}\end{aligned} \tag{6.11}$$

$J(\mathbf{h})$ が極値をとるときの $\mathbf{h}$ を求めればよいので、$J(\mathbf{h})$ を $\mathbf{h}$ で微分したものが 0 になるとすると、

$$\nabla_h\left[J(\mathbf{h})\right]=2\frac{\mathbf{h}^{*}\mathbf{m}\mathbf{m}^{*}\mathbf{h}}{\mathbf{h}^{*}(\mathbf{S}+\mathbf{C})\mathbf{h}}-2\frac{\left(\mathbf{h}^{*}\mathbf{m}\mathbf{m}^{*}\mathbf{h}\right)(\mathbf{S}+\mathbf{C})\mathbf{h}}{\left[\mathbf{h}^{*}(\mathbf{S}+\mathbf{C})\mathbf{h}\right]^2}=\mathbf{0} \tag{6.12}$$

となる。これを簡単にすると、

$$\frac{1}{\mathbf{h}^{*}(\mathbf{S}+\mathbf{C})\mathbf{h}}\left[\mathbf{m}\mathbf{m}^{*}\mathbf{h}-\lambda(\mathbf{S}+\mathbf{C})\mathbf{h}\right]=\mathbf{0} \tag{6.13}$$

となる。ここで、

$$\lambda = \frac{\mathbf{h}^* \mathbf{m}\mathbf{m}^* \mathbf{h}}{\mathbf{h}^* (\mathbf{S}+\mathbf{C})\mathbf{h}} = J(\mathbf{h}) \tag{6.14}$$

である。式(6.13)の括弧内が 0 になればよいので、

$$\mathbf{m}\mathbf{m}^*\mathbf{h} - \lambda(\mathbf{S}+\mathbf{C})\mathbf{h} = \mathbf{0} \tag{6.15}$$

$$(\mathbf{S}+\mathbf{C})^{-1}\mathbf{m}\mathbf{m}^*\mathbf{h} = \lambda\mathbf{h} \tag{6.16}$$

となる。式(6.15)から式(6.16)に変換した際、$(\mathbf{S}+\mathbf{C})$ は正則行列だと仮定している。また、式(6.15)は固有値の問題である。$(\mathbf{S}+\mathbf{C})$ が正則行列の場合、$\mathbf{h}$は$(\mathbf{S}+\mathbf{C})^{-1}\mathbf{m}\mathbf{m}^*$の固有ベクトルでなくてはならない。$\lambda$ は $J(\mathbf{h})$ と等しいため、λ が最大となるような固有ベクトルを選択すればよい。一般的に、フルランクの $d \times d$ の行列は d 個の 0 でない固有値をもつ。しかし、$\mathbf{m}\mathbf{m}^*$ はベクトルの直積であるため、ランクは 1 となり、$(\mathbf{S}+\mathbf{C})^{-1}\mathbf{m}\mathbf{m}^*$は 1 つしか 0 でない固有値をもたない。よって、(6.16)において $\mathbf{m}^*\mathbf{h} = \alpha$ (α はスカラー値)と置き換えることで、固有ベクトルは以下のように求められる。

$$\alpha(\mathbf{S}+\mathbf{C})^{-1}\mathbf{m} = \lambda\mathbf{h} \tag{6.17}$$

$$\mathbf{h} = c(\mathbf{S}+\mathbf{C})^{-1}\mathbf{m} \tag{6.18}$$

ここで、$c = \alpha/\lambda$ はスケールファクタである。

謝辞

本研究を進めるにあたり、御指導御鞭撻を賜りました山口雅浩教授に心から感謝の意を表します。

また学位論文の審査を引き受けて頂いた東京工業大学大学院総合理工学研究科物理情報システム専攻の小林隆夫教授、伊東利哉教授、熊澤逸夫教授、小尾高史准教授に心より感謝の意を表します。また熊澤逸夫教授には G-COE メンターとして研究について貴重なご意見を頂き大変勉強になりました。静岡大学工学部システム工学科の生源寺類講師には外部審査員を快く引き受けて頂き感謝の意を表します。

大山永昭教授、小尾高史准教授、村上百合特任助教、鈴木裕之助教には研究環境の提供及び研究の成果について有益なご助言やご討論いただきましたことを御礼申し上げます。日本体育大学助教中野和也さんには同じ研究分野の先輩として、研究内容の討論など、様々な面でご協力頂きました。

木村文一研究員、石川雅浩助教、Sercan Taha Ahi 元研究員には研究者の先輩として様々なアドバイスを頂きましたことに感謝の意を表します。山口研究室秘書の大川みのりさん、大山研究室秘書の黒田京香さんには様々な手続きなどご支援を頂き、感謝の意を表します。またご卒業された方々を含めた山口研究室、大山研究室、小尾研究室の学生の皆様には研究面、生活面で多大なご協力を賜りましたことを深く感謝致します。

アメリカ合衆国・ミシガン州立大学の Arun Ross 准教授には、留学の受入と研究についてのディスカッションをさせていただいたことに感謝の意を表します。また、Asem Othman 研究員や Ajita Rattani 研究員には研究のディスカッションだけでなく、アメリカでの暮らしをサポートしていただきましたことを御礼申し上げます。同研究室の皆様には、これまでとは異なった視点からの研究のディスカッションをさせていただいたことに感謝いたします。

本研究は「グローバル COE プログラムフォトニクス集積コアエレクトロニクス」及び「博士一貫教育プログラム」の支援の下に行われました。国際会議参加への渡航援助等、様々なご支援頂きましたことに感謝致します。ミシガン州立大学への留学の際に、「博士一貫教育プログラム」に渡航費や生活費等のご支援をいただきましたことに感謝致します。

参考文献

[1] S. Platform, “バイオメトリクスセキュリティ の課題 小松 尚久 Japanese standardization activities related to biometrics Security 類似度の分布,” 2006.

[2] 大山永昭, “次世代 IC カードシステムと暗号技術(<小特集>明るい社会を築く暗号： 暗号は社会を変革する),” 電子情報通信学会誌, vol. 83, no. 2, pp. 91–95, Feb. 2000.

[3] 瀬戸洋一, サイバーセキュリティにおける生体認証技術 [単行本]. .

[4] J. Daugman, “How Iris Recognition Works,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 21–30, Jan. 2004.

[5] J. Daugman, “IRIS RECOGNITION BORDER-CROSSING SYSTEM IN THE UAE,” *International Airport Review*, vol. 8, no. 2, 2004.

[6] 山田浩二, 松本弘之, and 松本勉, “ISEC2000-45 指紋照合装置は人工指を受け入れるか,” *電子情報通信学会技術研究報告. ISEC, 情報セキュリティ*, vol. 100, no. 213, pp. 159–166, Jul. 2000.

[7] D. Willis and M. Lee, “Six biometric devices point the finger at security,” *Network Computing*, vol. 9, no. 10, pp. 84–96, Jun. 1998.

[8] J. Domingo-Ferrer, D. Chan, and A. Watson, *Smart Card Research and Advanced Applications*. Boston, MA: Springer US, 2000.

[9] N. Delvaux, H. Chabanne, J. Bringer, B. Kindarji, P. Lindeberg, J. Midgren, J. Breebaart, T. Akkermans, M. V. Veen, R. Veldhuis, E. Kindt, K. Simoens, C. Busch, P. Bours, D. Gafurov, B. Yang, J. Stern, C. Rust, B. Cucinelli, and D. Skepastianos, “Pseudo Identities Based on Fingerprint Characteristics,” *2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 1063–1068, Aug. 2008.

[10] P. Refregier, “Optical image encryption based on input plane,” *Optics Letters*, vol. 20, no. 7, pp. 767–769, 1995.

[11] B. Javidi and J. L. Horner, “Optical pattern recognition for validation and security verification,” in *SPIE’s International Symposium on Optical Engineering and Photonics in Aerospace Sensing*, 1994, pp. 224–230.

[12] H. Suzuki, M. Yamaguchi, M. Yachida, N. Ohyama, H. Tashima, and T. Obi, “Experimental evaluation of fingerprint verification system based on double random phase encoding.,” *Optics express*, vol. 14, no. 5, pp. 1755–66, Mar. 2006.

[13] N. OTSU, “A Tlreshold Selection Method from Gray-Level Histograms,” *Automatica*, vol. 11, pp. 285–296, 1975.

[14] F. Wyrowski and O. Bryngdahl, “Iterative Fourier-transform algorithm applied to computer holography,” *Journal of the Optical Society of America A*, vol. 5, no. 7, p. 1058, Jul. 1988.

[15] a Mahalanobis, B. V Kumar, and D. Casasent, “Minimum average correlation energy filters.,” *Applied optics*, vol. 26, no. 17, pp. 3633–40, Sep. 1987.

[16] A. Mahalanobis, H. Missile, S. Company, and B. V. K. V. Kumar, “Optimality of the maximum average correlation height filter for detection of targets in noise”, Optics Engineering, vol. 36(10), 2642-2648, 1997.

[17] B. V. K. Vijaya Kumar, M. Savvides, C. Xie, K. Venkataramani, J. Thornton, and A. Mahalanobis, “Biometric verification with correlation filters.,” *Applied optics*, vol. 43, no. 2, pp. 391–402, Jan. 2004.

[18] “FVC2000 Technical Report.” [Online]. Available: http://bias.csr.unibo.it/fvc2000/download.asp. [Accessed: 27-Jan-2014].

[19] “Peter’s Functions for Computer Vision.” [Online]. Available: http://www.csse.uwa.edu.au/~pk/research/matlabfns/#fingerprints. [Accessed: 09-Feb-2014].

[20] K. Nilsson and J. Bigun, “Localization of corresponding points in fingerprints by complex filtering,” *Pattern Recognition Letters*, vol. 24, no. 13, pp. 2135–2144, Sep. 2003.

[21] “FVC2000.” [Online]. Available: http://bias.csr.unibo.it/fvc2000/results.asp. [Accessed: 10-Feb-2014].

[22] Y. Rachlin and D. Baron, “The secrecy of compressed sensing measurements,” *2008 46th Annual Allerton Conference on Communication, Control, and Computing*, pp. 813–817, Sep. 2008.

[23] H. Suzuki, M. Suzuki, T. Urabe, T. Obi, M. Yamaguchi, and N. Ohyama, “Secure biometric image sensor and authentication scheme based on compressed sensing,” *Applied Optics*, vol. 52, no. 33, p. 8161, Nov. 2013.

[24] P. Clemente, V. Durán, V. Torres-Company, E. Tajahuerce, and J. Lancis, “Optical encryption based on computational ghost imaging.,” *Optics letters*, vol. 35, no. 14, pp. 2391–3, Jul. 2010.

[25] 矢野佑樹, 仁田功一, 的場修, “レーザーアレイを用いたゴーストイメージング,” Optics & Photonics Japan 講演予稿集(CD-ROM), vol. 2011, 2011.

[26] J. Romberg and M. Wakin, “Compressed Sensing：A Tutorial Shannon / Nyquist sampling theorem – no information loss if we sample at 2x signal bandwidth Data Acquisition DSP・revolution：Increasing pressure on DSP hardware , algorithms,” 2007.

[27] O. V Holtz, U. C. Berkeley, and T. U. Berlin, “An Introduction to Compressive Sensing Compressed Sensing：History Compressed Sensing (CS),” no. January, 2009.

[28] D. L. Donoho, “Compressed sensing,” *IEEE Transactions on Information Theory*, vol. 52, no. 4, pp. 1289–1306, Apr. 2006.

[29] D. Gabor, “A New Microscopic Principle.pdf.” Nature, p. 777, 1948.

[30] J. W.Goodman, 尾崎義治, 朝倉利光, フーリエ光学 [単行本(ソフトカバー)]. .

[31] T. Utsugi and M. Yamaguchi, “Reduction of the recorded speckle noise in holographic 3D printer,” *Optics Express*, vol. 21, no. 1, p. 662, Jan. 2013.

[32] G. Schirripa Spagnolo and L. Cozzella, “Laser speckle decorrelation for fingerprint acquisition,” *Journal of Optics*, vol. 14, no. 9, p. 094006, Sep. 2012.

[33] M. Takeda, H. Ina, and S. Kobayashi, “Fourier-transform method of fringe-pattern analysis for computer-based topography and interferometry,” *Journal of the Optical Society of America*, vol. 72, no. 1, p. 156, Jan. 1982.

[34] B. Javidi, “Nonlinear joint power spectrum based optical correlation.”, Applied Optics, Vol. 28, Issue 12, pp. 2358-2367 (1989)

[35] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, “Physical one-way functions.,” *Science (New York, N.Y.)*, vol. 297, no. 5589, pp. 2026–30, Sep. 2002.

[36] Helinski, R., Acharyya, D. and Plusquellic, J. (2009) A Physical Unclonable Function Defined Using Power Distribution System Equivalent Resistance Variations. Proceedings of the 46th Annual Design Automation Conference on ZZZ-DAC’09, 676. http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5227103&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5227103

[37] R. Helinski, D. Acharyya, and J. Plusquellic, “A physical unclonable function defined using power distribution system equivalent resistance variations,” *Proceedings of the 46th Annual Design Automation Conference on ZZZ - DAC ’09*, p. 676, 2009.

[38] 高橋健太, 比良田真史, 三村昌弘, and 手塚悟, “セキュアなリモート生体認証プロトコルの提案,” 情報処理学会論文誌, vol. 49, no. 9, pp. 3016–3027, Sep. 2008.

[39] 柴田陽一, 中村逸一, 三村昌弘, 高橋健太, and 西垣正勝, “統計的 AD 変換による生体情報を用いた Challenge & Response 型ネットワーク認証の提案,” *情報処理学会研究報告. CSEC, [コンピュータセキュリティ]*, vol. 2004, no. 75, pp. 179–186, Jul. 2004.

[40] 森浩典, 鈴木裕之, 小尾高史, 山口雅浩, and 大山永昭, “M_048 生体情報を鍵とするチャレンジ&レスポンス型認証(M 分野:アーキテクチャ・ユビキタス・セキュリティ),” 情報科学技術フォーラム一般講演論文集, vol. 5, no. 4, pp. 301–302, Aug. 2006.

[41] “中国人が特殊なホログラムシール付きの外国人登録証明書を偽造！｜日本のお姉さん.” [Online]. Available: http://ameblo.jp/nyaonnyaon/entry-10005040784.html.

[42] “ばねをバネに新分野へ:NHK ニッパツ 日本発条株式会社｜STS 事業部 製品情報 偽造防止関連 トラストグラム.” [Online]. Available: http://www.nhkspg.co.jp/info-sec/jp/products/info/cpl.html.

[43] “3 次元 CG ホログラム『バーチャグラム(R)』の輝度を 2 倍にアップ ｜ DNP 大日本印刷株式会社.” [Online]. Available: http://www.dnp.co.jp/news/1229143_2482.html.

[44] “大日本印刷 アニメーションのように動くホログラム『モーションイマージュ ™』を開発 ｜ DNP 大日本印刷株式会社.” [Online]. Available: http://www.dnp.co.jp/news/1189520_2482.html.

[45] “凸版印刷/新しいセキュリティ技術「パールグラム」開発.” [Online]. Available: http://print-better.jagat.jp/story_memo_view.asp?StoryID=4982.

[46] “ばねをバネに新分野へ：NHK ニッパツ 日本発条株式会社｜STS 事業部 製品情報 偽造防止関連 アルタテックス.” [Online]. Available: http://www.nhkspg.co.jp/info-sec/jp/products/info/altattex.html.

[47] “DNA インキ CustoMerQ（カスタマーク） ｜ 日本写真印刷株式会社.” [Online]. Available: http://www.nissha.com/crd/customerq/index.html.

[48] “偽造防止ラベル FORGE GUARD®（フォージガード） ｜ 富士フイルム.” [Online]. Available: http://fujifilm.jp/business/security/anti_counterfeit/forge_guard/.

[49] “凸版印刷｜凸版印刷、世界初、半導体の個体差を用いた PUF 技術搭載 IC タグ「SMARTICS-V」による真贋判定サービスの提供を開始.” [Online]. Available: http://www.toppan.co.jp/news/2013/09/newsrelease130925.html.

研究業績

(博士論文に関する業績)

【学術論文】

- **Masafumi Takeda**, Kazuya Nakano, Hiroyuki Suzuki, Masahiro Yamaguchi, “Encoding plaintext by Fourier transform hologram in double random phase encoding using fingerprint keys,” Journal of Optics, **14**(2012), 094003.

- **Masafumi Takeda**, Kazuya Nakano, Hiroyuki Suzuki, Masahiro Yamaguchi, “Encrypted Sensing Based on Digital Holography for Fingerprint Images”, Optics and Photonics Journal (OPJ), 2015, **5**, No.1,

【国際会議(査読なし)】

- **Masafumi Takeda**, Hiroyuki Suzuki, Masahiro Yamaguchi, Takashi Obi, Nagaaki Ohyama. “Shift and Rotation Invariant Double Random Phase Encoding Using Fingerprint Keys”, Frontiers in Optics (FiO) 2010, Frontiers in Optics (FiO) 2010 paper, FTuD6, Oct. 2010.

【国際会議(査読あり)】

- **Masafumi Takeda**, Kazuya Nakano, Hiroyuki Suzuki, Masahiro Yamaguchi, “Secure capture of biometric information using optical encryption”, Tokyo, Japan, 37th IEEE EDS WIMNACT, February 18, 2013, p-102

【国内学会・研究会】

- 竹田賢史, 鈴木裕之, 山口雅浩, 小尾高史, 大山永昭. “指紋を鍵とする暗号化手法における演算の高速化に関する検討”, 電子情報通信学会 2009 年総合大会, 電子情報通信学会 2009 年総合大会講演予稿集, B-18-1, p. 563, Mar. 2009

- 鈴木 裕之, 竹田 賢史, 山口 雅浩. 指紋を鍵とする暗号化手法における演算の高速化に関する検討, 第 3 回新画像システム・情報フォトニクス研究討論会, 第 3 回新画像システム・情報フォトニクス研究討論会講演予稿集, B-3, pp. 30-31, May. 2009.

- 竹田賢史, 鈴木裕之, 山口雅浩, 小尾高史, 大山永昭. “指紋を鍵とする暗号化手法における平文画像のコーディング方法に関する検討”, 第 70 回応用物理学会学術講演会, 第 70 回応用物理学会学術講演会講演予稿集, Vol. 3, 11a-D-8, p. 925, Sep. 2009

- 竹田 賢史, 鈴木 裕之, 山口 雅浩, 小尾 高史, 大山 永昭. “指紋の位置・回転に対して不変な二重ランダム位相暗号化手法”, バイオメトリックシステムセキュリティ研究会第 21 回研究会, バイオメトリックシステムセキュリティ研究会第 21 回研究会予稿集, pp. 7-12, Mar. 2010.

- 鈴木 裕之, **竹田 賢史**, 山口 雅浩, 小尾 高史, 大山 永昭. 生体情報を鍵とする二重ランダム位相暗号化における平文コーディング方法の改善, SCI2010(暗号と情報セキュリティシンポジウム), SCI2010(暗号と情報セキュリティシンポジウム)予稿集, 2F1-1, Jan. 2010.

- **竹田賢史**，中野和也，鈴木裕之，山口雅浩，” デジタルホログラフィーを用いた秘匿化生体情報取得と照合に関する研究”, 2013 年暗号と情報セキュリティシンポジウム（SCIS2013）, 3D2-2, 京都市, 2013 年 1 月

- **竹田賢史**，中野和也，鈴木裕之，山口雅浩，” ディジタルホログラフィーを用いた生体情報の秘匿化センシング”, 第 60 回応用物理学春季学術講演会，29p-A1-2，神奈川工科大学，2013 年 3 月，講演予稿集 p.03-074

- **竹田賢史**，中野和也，鈴木裕之，山口雅浩，” ディジタルホログラフィーを用いた秘匿化センシングによる生体情報の取得”, 平成 25 年第 2 回ホログラフィックディスプレイ研究会, 電気通信大学, 2013 年 5 月，会報, Vol.33, No.2, pp.25-29

- 鈴木裕之, **竹田賢史**, 中野和也, 山口雅浩. ディジタルホログラフィーを用いた指紋画像秘匿化センサー, 第 7 回新画像システム・情報フォトニクス研究討論会, 第 7 回新画像システム・情報フォトニクス研究討論会予稿集, pp. 62-63, Jun. 2013.

【表彰】

- 37th IEEE EDS WIMNACT, Best Poster Award, February 18, 2013

(その他の業績)

【学術論文】

- Hideaki Tashima, **Masafumi Takeda**, Hiroyuki Suzuki, Takashi Obi, Masahiro Yamaguchi, Nagaaki Ohyama, “Known plaintext attack on double random phase encoding using fingerprint as key and a method for avoiding the attack”, Optics Express, Vol. 18, No. 13, pp. 13772-13781, Jun. 2010.

- Kazuya Nakano, **Masafumi Takeda**, Hiroyuki Suzuki, Masahiro Yamaguchi, “Generalized

Model of Double Random Phase Encoding Based on Linear Algebra," Optics communications , Volume 286, 1 January 2013, Pages 91–94.

- Kazuya Nakano, **Masafumi Takeda**, Hiroyuki Suzuki, Masahiro Yamaguchi, "Evaluations of Phase-only double random phase encoding based on key-space analysis," Applied optics, Vol. 52, No.6, 20, February 2013

【国際会議(査読あり)】

- Hiroyuki Suzuki, Shizuo Sakamoto, Takashi Miyai, Kazuya Nakano, **Masafumi Takeda**. "A novel framework for evaluation of ID photo quality," International Biometric Performance Testing Conference 2012 (IBPC2012), Mar. 2012.

【国内学会・研究会】

- 中野和也, 鈴木裕之, 山口雅浩, **竹田賢史**. 二重ランダム位相暗号化法に対する既知平文攻撃の定量分析, Optics & Photonics Japan 2011, Optics & Photonics Japan 2011 講演予稿集, Nov. 2011.

- 鈴木裕之, 坂本静生, 宮井貴志, 中野和也, **竹田賢史**, 鈴木理道, 前田大輔. ID 用顔画像の品質評価用フレームワークの提案, 第 10 回情報科学技術フォーラム(FIT2011), 第 10 回情報科学技術フォーラム講演論文集, N-033, pp. 489-490, Sep. 2011.

- 中野 和也, **竹田賢史**, 鈴木 裕之, 山口 雅浩, "代数学的表現による二重ランダム位相暗号化法の一般化," 第６回新画像システム･情報フォトニクス研究討論会, 第６回新画像システム・情報フォトニクス研究討論会講演予稿集, pp. 65-66, June. 2012.

- 中野和也, 鈴木裕之, 山口雅浩, **竹田賢史**. "二重ランダム位相暗号化法に対する既知平文攻撃の解読可能性に関する検討," レーザー学会学術講演会第 32 回年次大会, レーザー学会学術講演会第 32 回年次大会講演予稿集, Jan. 2012.

- 中野和也, 鈴木裕之, 山口雅浩, **竹田賢史**. "二重ランダム位相暗号化法に対する既知平文攻撃の定量分析," Optics & Photonics Japan 2011, Optics & Photonics Japan 2011 講演予稿集, Nov. 2011.

- 中野和也，**竹田賢史**，鈴木裕之，山口雅浩．インテグラルフォトグラフィーに基づいた秘匿化イメージング，第 7 回新画像システム・情報フォトニクス研究討論会，第 7 回新画像システム・情報フォトニクス研究討論会予稿集, pp. 34-35, Jun. 2013.

- 中野和也，**竹田賢史**，鈴木裕之，山口雅浩．二重ランダム位相暗号化法の評価及び拡張性についての研究，第 14 回情報フォトニクス研究グループ研究会，第 14 回情報フォトニクス研究グループ研究会予稿集, pp. 40-45, Sep. 2013.